Th des 2 carrés

→ $\mathbb{Z}[i]$, norme, inversibles

→ Prq $p = a^2 + b^2$ ssi p réductible dans $\mathbb{Z}[i]$ (avec norme)

→ Prq p réductible dans $\mathbb{Z}[i]$ ssi -1 carré modulo p (avec correspondance des idéaux)

→ Prq Σ multiplicative, et pgcd pour réciproque.

Prérequis

- $\mathbb{Z}[i]$ euclidien
- implications euclidien, ppal, factoriel
- carrés dans $\overline{\mathbb{F}_p}$
- correspondance des idéaux

Théorème des deux carrés

Perrin

DEV

Théorème

Soit $p \geq 3$ premier.

On pose $\Sigma := \{\text{somme de deux carrés}\} = \{a^2+b^2,\ a,b \in \mathbb{N}\}$.

Alors $(p \in \Sigma) \iff (p \equiv 1\ [4])$

preuve

- On se place dans l'anneau des entiers de Gauss : $\mathbb{Z}[i]$. ⊛

On pose : $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$, $a+ib \longmapsto a^2+b^2$

- N est multiplicative : $\forall z, z' \in \mathbb{Z}[i]$, $N(zz') = |zz'|^2 = |z|^2|z'|^2 = N(z)N(z')$
- $\mathbb{Z}[i]^\times = \{\pm 1; \pm i\} = \{z \in \mathbb{Z}[i] \text{ tq } N(z) = 1\}$

  En effet : . ces 4 éléments sont inversibles

  . Soit $z \in \mathbb{Z}[i]^\times$ Alors $zz^{-1} = 1$ et $\underbrace{N(z)}_{\in \mathbb{Z}} \underbrace{N(z^{-1})}_{\in \mathbb{Z}} = 1$.

  donc $N(z) = \pm 1$ mais positive, donc $N(z) = 1 = a^2+b^2$.

  Donc couples possibles : $(1,0), (-1,0), (0,1), (0,-1)$.

- TCq $p \in \Sigma$ ssi p est réductible dans $\mathbb{Z}[i]$

⟹ Supposons $p = a^2+b^2 \in \Sigma$. Alors $p = N(a+ib) = (a+ib)(a-ib)$

et $N(a+ib) = p > 1$ donc $a+ib$ non inversible ($a-ib$ non plus pour les mêmes raisons)

Donc p est réductible dans $\mathbb{Z}[i]$.

⟸ Supposons p réductible : $p = zz'$ dans $\mathbb{Z}[i]$, z et $z' \notin \mathbb{Z}[i]^\times$

Alors $N(zz') = N(p) = p^2$

$N(z)N(z')$

Donc $N(z) \mid p^2$. Comme p premier, $N(z) \mid p$ et comme z non inversible, $N(z) = p$.

Donc $p \in \Sigma$ en tant que norme d'un élément de $\mathbb{Z}[i]$.

• À quelle condition p est-il réductible dans $\mathbb{Z}[i]$?

× $\mathbb{Z}[i]$ est factoriel ⊛ (donc irréductible = premier)

Donc p réductible dans $\mathbb{Z}[i]$ ssi (p) pas un idéal premier de $\mathbb{Z}[i]$

ssi $\mathbb{Z}[i]/(p)$ non intègre

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

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

⊛

Donc on cherche à quelle condition $\mathbb{F}_p[X]/(X^2+1)$ n'est pas intègre ie à quelle condition X^2+1 n'est pas premier, ie pas réductible car $\mathbb{F}_p[X]$ est factoriel.

Or, X^2+1 réductible dans $\mathbb{F}_p[X]$ ssi a une racine dans $\mathbb{F}_p[X]$

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

ssi $(-1)^{\frac{p-1}{2}} = 1$ ie $p \equiv 1\ [4]$ ▨

Corollaire

Pour $n \in \mathbb{N}^*$, on a $(n \in \Sigma) \iff (v_p(n) \text{ impaire} \Rightarrow p \equiv 1\ [4])$

preuve

• Σ est stable par multiplication :

$n \in \Sigma$ ssi $\exists\, z \in \mathbb{Z}[i]$ tq $n = N(z)$

Donc si $n, m \in \Sigma$, $nm = N(z)N(z') = N(zz') \in \Sigma$.

$\Leftarrow$ Soit $n \in \mathbb{N}^*$.

Si $\exists p$ tq $v_p(n)$ impaire. Supposons $p \equiv 1\ [4]$.

Alors $n = \left(\prod_{\substack{p \in \mathcal{P} \\ v_p(n) \text{ paire}}} p^{\frac{v_p(n)}{2}} \right)^2 \cdot \underbrace{\prod_{\substack{p \in \mathcal{P} \\ v_p(n) \text{ paire}}} p^{v_p(n)}}_{\text{produit d'éléments de } \Sigma}$

donc $n \in \Sigma$

$\Rightarrow$ Soit $n \in \Sigma$. $n = a^2+b^2$ on note $d = a \wedge b$ et $a = a'd$, $b = b'd$, $a' \wedge b' = 1$

Alors $n = d^2(a'^2 + b'^2)$

Soit $p \in \mathcal{P}$ un facteur premier de n à valuation impaire.

Alors $p \mid n = d^2(a'^2+b'^2)$ et $p \nmid d$ sinon p serait à valuation paire.

Donc $p \mid a'^2+b'^2$ et comme $a' \wedge b' = 1$, $p \nmid a'$ et $p \nmid b'$

En particulier, a' est inversible dans $\mathbb{Z}/p\mathbb{Z}$ (enfin sa classe).

$$a'^2+b'^2 = 0 = a'^2(1 + a'^{-2}b'^2)$$ or par intégrité de $\mathbb{Z}/p\mathbb{Z}$,

$$a'^{-2}b'^2 = -1.$$

Donc -1 est un carré dans $\mathbb{F}_p$, donc $p \equiv 1 \ [4]$.

□

Parenthèse : Anneau de Gauss $\mathbb{Z}[i]$

- $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$, donc il est intègre.
- $\mathbb{Z}[i]$ est euclidien :

  Soit $z, t \in \mathbb{Z}[i]$, $t \neq 0$. $\frac{z}{t} \in \mathbb{C}$ donc il existe $x, y \in \mathbb{R}$ tels que $\frac{z}{t} = x + iy$.

  On pose a, b les entiers les plus proches de x et y. et $q = a+ib$.

  On pose $r = z - qt$.

  Alors $|r| = |t|\left|\frac{z}{t} - q\right| = |t|\sqrt{|x-a|^2 + |y-b|^2}$. Mais $|x-a| \leq \frac{1}{2}$, $|y-b| \leq \frac{1}{2}$

  Donc $|r| \leq |t|\frac{\sqrt{2}}{2} < |t|$. D'où la division euclidienne avec $N(r) < N(t)$.

  □

- Donc $\mathbb{Z}[i]$ est factoriel et on a toujours premier $\Rightarrow$ irréductible, et c'est une caractéristique d'un anneau factoriel - avec la décomposition - d'avoir la réciproque. Donc irréductible $\Leftrightarrow$ premier dans $\mathbb{Z}[i]$.

- On a l'isomorphisme $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$

  En effet, on considère le morphisme d'anneaux $\mathbb{Z}[X] \longrightarrow \mathbb{Z}[i]$, $P \longmapsto P(i)$

  X^2+1 est irréductible sur $\mathbb{Z}$ (pas de racines) et annule i sur $\mathbb{C}$. Donc engendre le noyau du morphisme. D'où l'isomorphisme.

[ULMER]

Théorème d'isomorphisme :

$f : A \longrightarrow B$ morphisme d'anneaux

$I = \ker f$

Soit J idéal de A contenu dans I, et p la surjection canonique.

Alors $\exists ! \bar{f} : A/J \longrightarrow B$ tq $f = \bar{f} \circ p$.

Correspondance des idéaux

Soit $\varphi : A \longrightarrow B$ morphisme d'anneaux surjectif, de noyau J

1. Idéal de A contenant J $\longleftrightarrow$ Idéal de B

$$I \overset{\alpha}{\longmapsto} \varphi(I)$$
$$\varphi^{-1}(H) \overset{\beta}{\longleftarrow} H$$

α, β bijections réciproques l'une de l'autre.

2. Si deux idéaux se correspondent, alors $A/I \longrightarrow B/H$, $a + I \longmapsto \varphi(a) + H$ est un isomorphisme d'anneaux.

preuve

1. β bien définie : Soit H idéal de B. Alors $\varphi^{-1}(H)$ idéal de A ($x \in \varphi^{-1}(H)$, $a \in A$

$\varphi(xa) = \varphi(x)\underbrace{\varphi(a)}_{\in B} \in H$ donc $xa \in \varphi^{-1}(H)$) qui contient J (H contient 0 car c'est un idéal de B, donc $J = \varphi^{-1}(\{0\}) \in \varphi^{-1}(H)$).

α bien définie : φ est surjective donc $\varphi(I)$ idéal de B : Soit $y \in \varphi(I)$ et $b \in B$.

$y = \varphi(\underbrace{x}_{\in I})$ $b = \varphi(a)$ car surj, $yb = \varphi(\underbrace{ax}_{\in I}) \in \varphi(I)$ et ssgpe car non vide (contient 0) et φ morphisme.

$\alpha \circ \beta = id$: Soit H idéal de B. $\alpha \circ \beta(H) = \varphi(\varphi^{-1}(H))$

On a $\varphi(\varphi^{-1}(H)) \subset H$ par def.

Soit $y \in H$. φ surjective donc $\exists x \in A$ tq $y = \varphi(x)$. Alors $x \in \varphi^{-1}(H)$ et $y \in \varphi(\varphi^{-1}(H))$

$\beta \circ \alpha = id$: Soit I idéal de A contenant J. $\beta \circ \alpha(I) = \varphi^{-1}(\varphi(I))$

On a $I \subset \varphi^{-1}(\varphi(I))$

Soit $x \in \varphi^{-1}(\varphi(I))$. Alors $\varphi(x) \in \varphi(I)$ donc $\exists y \in I$ tq $\varphi(x) = \varphi(y)$ ie $\varphi(x-y) = 0$ ie $x - y \in J \subset I$ donc $x \in y + I = I \longrightarrow x \in I$.

2. $B \longrightarrow B/H$ morphisme surjectif canonique $A \overset{\varphi}{\longrightarrow} B \overset{\pi}{\longrightarrow} B/H$

$\pi \circ \varphi$ surjectif. et $\ker(\pi \circ \varphi) = \varphi^{-1}(\ker \pi) = \varphi^{-1}(H) = I$.

Donc $A/I \simeq B/H$.

De cette correspondance des idéaux on déduit que pour A anneau,
I, J idéaux de A,

$$(A/I)/\overline{J} \simeq (A/J)/\overline{I}$$

En effet, on prouve que $(A/I)/\overline{J} \simeq A/(I,J) \simeq (A/J)/\overline{I}$

$\pi : A \longrightarrow A/I$ morphisme surjectif

$\overline{J}$ idéal de A/I qui correspond à (I,J), idéal de A contenant I

Donc $A/(I,J) \simeq (A/I)/\overline{J}$

D'où, dans notre cas, $\left(\mathbb{Z}[X]/(X^2+1)\right)/\overline{(p)} \simeq \mathbb{Z}[X]/(p, X^2+1) \simeq \mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$