[Perrin p. 56]

leçons 126
121
122

Théorème des deux carrés de Fermat :

Il faudra préalablement avoir placé dans la leçon :

- inversibles de $\mathbb{Z}[i]$ (norme "arithmétique")
- $\mathbb{Z}[i]$ euclidien donc principal

Et il faut écrire en intro au développement :

Définition : On pose $\Sigma = \{ n \in \mathbb{N} \; ; \; n = a^2 + b^2, (a,b) \in \mathbb{N}^2 \}$ l'ensemble des entiers qui sont sommes de deux carrés.

Prop : Σ est stable par multiplication.

(En effet, $n \in \Sigma \Leftrightarrow \exists z \in \mathbb{Z}[i]$ tq $n = N(z)$, puis on utilise la multiplicativité de la norme).

Le développement

Lemme : $p \in \Sigma \Leftrightarrow p$ n'est pas irréductible dans $\mathbb{Z}[i]$

Preuve : $\boxed{\Rightarrow}$ $p \in \Sigma \Rightarrow p = a^2 + b^2$, $(a,b) \in \mathbb{N}^2$

$$\Rightarrow p = \underbrace{(a+ib)(a-ib)}_{\text{de norme } p}$$

et c'est donc une décomposition non banale par caractérisation des irréductibles (càd ils sont de norme 1).

donc p n'est pas irréductible.

$\boxed{\Leftarrow}$ Soit $p = z . z'$ une décomposition non banale de p.

$\underbrace{N(p)}_{= p^2} = N(z) . N(z')$ avec $N(z)$ et $N(z') \neq 1$.

Ainsi $p = N(z)$ et donc $p = a^2 + b^2$ pour $z = a + ib$.

Ainsi $p \in \Sigma$.

Ce lemme est utile pour prouver le

<u>Théorème</u> : Soit p premier. $p \in \Sigma \Leftrightarrow p = 2$ ou $p \equiv 1$ $[4]$

<u>Preuve</u> : $\boxed{\Rightarrow}$ (contraposée)

Supposons $p \neq 2$ <u>et</u> $p \not\equiv 1$ $[4]$. Alors $p \equiv 3$ $[4]$ car un nombre premier différent de 2 est impair donc $\not\equiv 0$ $[4]$, $\not\equiv 2$ $[4]$

Or $q \in \Sigma \Leftrightarrow q = a^2 + b^2$ $(a,b) \in \mathbb{N}^2$

- si a pair, $a^2 \equiv 0$ $[4]$
- si a impair, $a^2 \equiv 1$ $[4]$

donc $a^2 + b^2 \equiv \begin{cases} 0 \\ 1 \\ 2 \end{cases}$ $[4]$

donc $p \notin \Sigma$ car $p \equiv 3$ $[4]$

inutile mais sympa à avoir sous la main

$\boxed{\Leftrightarrow}$ ▶ Mq $p \in \Sigma \Leftrightarrow -1$ carré dans $\mathbb{F}_p^*$

$\mathbb{Z}[i]$ principal donc p non irréductible $\Leftrightarrow p$ non premier

$\Leftrightarrow (p)$ non premier

$\Leftrightarrow \dfrac{\mathbb{Z}[i]}{(p)}$ non intègre

De plus $\mathbb{Z}[i] \simeq \dfrac{\mathbb{Z}[X]}{(X^2+1)}$ (thm de factorisation, voir TD)

donc $\dfrac{\mathbb{Z}[i]}{(p)} \simeq \dfrac{\mathbb{Z}[X]}{(p, X^2+1)} \simeq \dfrac{\frac{\mathbb{Z}}{p\mathbb{Z}}[X]}{(X^2+1)} \simeq \dfrac{\mathbb{F}_p[X]}{(X^2+1)}$ $\leftarrow \varphi : \frac{\mathbb{Z}}{p\mathbb{Z}[X]} \to \frac{\mathbb{Z}[i]}{p\mathbb{Z}[i]}$, $p \mapsto \overline{p(i)}$

et $\dfrac{\mathbb{F}_p[X]}{(X^2+1)}$ non intègre $\Leftrightarrow (X^2+1)$ non premier

$\Leftrightarrow X^2+1$ non premier de $\mathbb{F}_p[X]$

$\mathbb{F}_p[X]$ euclidien donc principal $\Leftrightarrow X^2+1$ non irréductible de $\mathbb{F}_p[X]$

$\Leftrightarrow -1$ carré de $\mathbb{F}_p^*$

▶ Mq -1 carré de $\mathbb{F}_p^* \Leftrightarrow p \equiv 1$ $[4]$ ou $p = 2$

- si $p = 2$, dans $\mathbb{F}_2^*$: $1^2 = 1 = -1$ donc -1 est un carré de $\mathbb{F}_2^*$.

  Donc on a bien le théorème.

- si $p > 2$

▶ Mq -1 carré dans $\mathbb{F}_p^*$ $\Leftrightarrow (-1)^{\frac{p-1}{2}} = 1$

<u>idée :</u> mq $\{x \in \mathbb{F}_p^* ;\ x \text{ carré de } \mathbb{F}_p^*\} = \{x \in \mathbb{F}_p^* ;\ x^{\frac{p-1}{2}} = 1\}$

Soit $x = y^2 \in \mathbb{F}_p^*$. On a alors $x^{\frac{p-1}{2}} = y^{p-1} = 1$

donc $\{x \in \mathbb{F}_p^* ;\ x \text{ carré de } \mathbb{F}_p^*\} \subset \{x \in \mathbb{F}_p^* ;\ x^{\frac{p-1}{2}} = 1\}$

De plus, $\#\{x \in \mathbb{F}_p^* ;\ x^{\frac{p-1}{2}} = 1\} \leq \frac{p-1}{2}$ ← ? car dans un corps, nbre de racine max du pol $X^{\frac{p-1}{2}} - 1$

(Nous allons mq $|\{x \in \mathbb{F}_p^* ;\ x \text{ carré de } \mathbb{F}_p^*\}| = \frac{p-1}{2}$

On définit $\varphi : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$
$x \longmapsto x^2$

$\mathrm{Im}\ \varphi = \{x \in \mathbb{F}_p^* ;\ x \text{ carré de } \mathbb{F}_p^*\}$

$\ker\ \varphi = \{\pm 1\}$

et on a le théorème d'isomorphisme : $\frac{|\mathbb{F}_p^*|}{|\ker(\varphi)|} = |\mathrm{Im}\ \varphi| = \frac{p-1}{2}$

Ainsi les deux ensembles étudiés sont de même cardinal et sont donc égaux.

On a donc -1 carré de $\mathbb{F}_p^*$ $\Leftrightarrow (-1)^{\frac{p-1}{2}} = 1$

$\Leftrightarrow \exists k \in \mathbb{Z} ;\ \frac{p-1}{2} = 2k$

$\Leftrightarrow \exists k \in \mathbb{Z} ;\ p = 4k+1$

$\Leftrightarrow p \equiv 1\ [4]$

▨

Après le développement :

(on peut rajouter le 1^er thm au dev si on est rapide)

Théorème : Soit $n \in \mathbb{N} \setminus \{0,1\}$. On décompose n en facteurs premiers $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$. Alors $n \in \Sigma \iff v_p(n)$ pair pour $p \equiv 3\ [4]$

$\boxed{\Leftarrow}$ On écrit $n = \underbrace{\Big(\prod_{\substack{p \in \mathcal{P} \\ p \equiv 3 [4]}} p^{\frac{v_p(n)}{2}} \Big)^2}_{\text{carré parfait}} \cdot \underbrace{\Big(\prod_{\substack{p \in \mathcal{P} \\ p \not\equiv 3 [4]}} p^{v_p(n)} \Big)}_{\substack{\text{produit de carrés parfaits par thm} \\ \text{précédent donc } \in \Sigma \text{ car } \Sigma \text{ stable mult.}}}$

$p \not\equiv 3[4]$ c.à.d $\begin{cases} p \equiv 1\ [4] \\ \text{ou} \\ p = 2 \end{cases}$

donc $n \in \Sigma$ (car $a^2 \cdot (x^2+y^2) = a^2x^2 + a^2y^2 = (ax)^2 + (ay)^2$)

$\boxed{\Rightarrow}$ Soit $n = a^2 + b^2 \in \Sigma$.

Notons $\delta = a \wedge b$, $a' = \frac{a}{\delta}$, $b' = \frac{b}{\delta}$ $\quad a' \wedge b' = 1$ et $n = \delta^2 (a'^2 + b'^2)$

Soit p un diviseur premier $\neq 2$ de $a'^2 + b'^2$. idée : Mq $p \equiv 1\ [4]$

ou δ en fiche de 2, il n'est pas concerné par ce qu'on veut montrer

et donc que $\{p \mid n$ et $p \equiv 3\ [4]\} \Rightarrow p \mid \delta^2$ donc d'exposant pair.

▶ Mq p réductible dans $\mathbb{Z}[i]$.

(absurde) Supposons p irréductible dans $\mathbb{Z}[i]$.

$p \mid a'^2 + b'^2 \Rightarrow p \mid (a'+ib')(a'-ib') \underset{\uparrow}{\Rightarrow} p$ divise un des facteurs

p divise aussi dans $\mathbb{Z}[i]$ — lemme Euclide

or l'un est conjugué de l'autre donc en passant au conjugué :

$\begin{cases} p \mid a'+ib' \\ \text{et} \\ p \mid a'-ib' \end{cases}$ donc $\begin{cases} p \mid 2a' \\ p \mid 2ib' \end{cases}$ donc $\begin{cases} p^2 \mid 4a'^2 \\ p^2 \mid 4b'^2 \end{cases} \underset{\substack{\uparrow \\ p \text{ impair}}}{\text{donc}} \begin{cases} p \mid a' \\ p \mid b' \end{cases}$

mais $a' \wedge b' = 1$... Contradiction ! Donc p non irréductible dans $\mathbb{Z}[i]$

▶ Donc $p = xy$, décomp <u>non</u> banale dans $\mathbb{Z}[i]$

donc $\underset{p^2}{N(p)} = \underset{\neq 1}{N(x)} \underset{\neq 1}{N(y)}$ et donc $N(x) = N(y) = p$. Donc $p \in \Sigma$

donc $p \equiv 1\ [4]$ par le théorème.

↳ Ainsi, tout facteur premier de n tq $p \equiv 3[4]$ divise le δ^2, et est donc d'exposant pair.

Prérequis :

Lemme: $\mathbb{Z}[i]$ euclidien et $\mathbb{Z}[i]^\times = \{\pm 1 ; \pm i\}$

▶ Posons $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$
$z = a+ib \longmapsto a^2 + b^2$

Soit $z, t \in \mathbb{Z}[i]$. On a $\frac{z}{t} = x + iy \in \mathbb{C}$

$\exists (a,b) \in \mathbb{Z}^2$ tq $|x-a| \leq \frac{1}{2}$ et $|y-b| \leq \frac{1}{2}$

Posons $q = a+ib \in \mathbb{Z}[i]$ et $r = z - qt$. On veut $N(r) < N(t)$. On a :

$|r| = |z - qt| = |t(\frac{z}{t} - q)| = |t| . |x+iy - (a+ib)|$
$= |t| \left((x-a)^2 + (y-b)^2 \right)^{1/2} \leq \frac{|t|}{\sqrt{2}} < |t|$

On obtient donc en passant au carré $N(r) = |r|^2 < |t|^2 = N(t)$. Ainsi N stathme. Ainsi $\mathbb{Z}[i]$ euclidien.

▶ $z = a+ib \in \mathbb{Z}[i]^\times$. Ainsi $\exists z' \in \mathbb{Z}[i]^\times$ tq $z.z' = 1$. On a donc $N(z).N(z') = 1$.
Or $N(z)$ et $N(z') \in \mathbb{N}$ donc $N(z)$ et $N(z') = 1$. Ainsi $a^2 + b^2 = 1$

Les seules solutions entières de cette équation sont $a = \pm 1$ et $b = 0$ <u>ou</u> $a = 0$ et $b = \pm 1$, d'où le résultat.