Développement : Théorème des deux carrés de Fermat

Algèbre & Géométrie

Références :
- [PER] Perrin D., *Cours d'algèbre*, ellipses, 1996, p56.
- [ROM] Rombaldi E., *Mathématiques pour l'agrégation : Algèbre et géométrie*, **2ème édition**, deobeck supérieur, 2021, p269.

Pour les leçons :
- 121 : Nombres premiers. Applications.
- 122 : Anneaux principaux. Exemples et applications.
- 127 : Exemples de nombres remarquables. Exemples d'anneaux de nombres remarquables. Applications.

Soit $\sum = \{n \in \mathbb{N} \mid \exists a, b \in \mathbb{N} \quad n = a^2 + b^2\}$. L'objectif de ce développement est de caractériser $\sum$.
On définit l'anneau des entiers de Gauss par $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ (on admettra ici que c'est bien un anneau).
On note enfin $\mathbb{P}$ l'ensemble des nombres premiers.

Lemme 1.

$\mathbb{Z}[i]$ est un anneau intègre principal et $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} = \{z \in \mathbb{Z}[i] \mid N(z) = 1\}$.

Preuve : On admet que $\mathbb{Z}[i]$ est un anneau (c'est du calcul). Il est intègre puisqu'inclus dans l'anneau intègre $\mathbb{C}$.
Soit $N : \mathbb{Z}[i] \to \mathbb{N}$ définie par :

$$\forall a + ib \in \mathbb{Z}(i) \quad N(a + ib) = a^2 + b^2.$$

N est en fait la restriction de $|\cdot|^2$ à $\mathbb{Z}[i]$. Montrons que $\mathbb{Z}[i]$ est euclidien pour l'application N.
Soient $z, t \in \mathbb{Z}[i]$ tels que $t \neq 0$. On écrit $\frac{z}{t} = x + iy$ avec $x, y \in \mathbb{R}$, et on se donne $q = a + ib \in \mathbb{Z}[i]$, où a et b sont des entiers choisis tels que $|x - a| \leqslant \frac{1}{2}$ et $|y - b| \leqslant \frac{1}{2}$. Posons $r = z - tq$, de sorte que $z = tq + r$.
Déjà, on remarque que $r = 0$ si, et seulement si $z = tq$, i.e. $a + ib = x + iy$, c'est-à-dire $x = a$ et $y = b$. Dans le cas contraire, on a $r \neq 0$ et :

$$\begin{aligned} N(r) &= |z - t(a + ib)|^2 \\ &= |t|^2 \left|\frac{z}{t} - (a + ib)\right|^2 \\ &= |t|^2 |(x - a) + i(y - b)|^2 \\ &= |t^2|((x - a)^2 + (y - b)^2) \\ &\leqslant |t|^2 \left(\frac{1}{4} + \frac{1}{4}\right) \\ &\leqslant \frac{|t|^2}{2} \\ &< N(t). \end{aligned}$$

$\mathbb{Z}[i]$ est donc euclidien (pour l'application N), donc principal.
Maintenant, soit $z \in \mathbb{Z}[i]$ inversible. Il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$.
Donc $N(z)N(z') = 1$. Comme $N(z)$ et $N(z')$ sont des entiers positifs, on a donc $N(z) = N(z') = 1$.
Enfin, en notant $z = a + ib$, avec $a, b \in \mathbb{Z}$, on a $1 = N(z) = a^2 + b^2$, donc $(a, b) \in \{(0, \pm 1), (\pm 1, 0)\}$, d'où le résultat. □

Lemme 2.

Soit $p \in \mathbb{P}$. Alors, $p \in \sum$ si, et seulement si p est réductible dans $\mathbb{Z}[i]$.

Preuve : Supposons $p \in \sum$. Il existe $a, b \in \mathbb{N}$ tels que $p = a^2 + b^2 = (a + ib)(a - ib)$.
a et b ne sont pas nuls : sinon, $p = a^2$ ou $p = b^2$, ce qui ne se peut puisque p est premier.
D'après le lemme précédent, on a donc $p \notin \mathbb{Z}[i]^\times$, et p n'est pas irréductible dans $\mathbb{Z}[i]$.

Réciproquement, supposons que p soit réductible dans $\mathbb{Z}[i]$. Il existe $z, z' \in \mathbb{Z}[i] \backslash \{\pm 1, \pm i\}$ tels que $p = zz'$.
Donc $p^2 = N(p) = N(z)N(z')$.
On a $N(z)$ et $N(z')$ non égaux à 1, par hypothèse sur z et z'. Donc $N(z) = N(z') = p$.
Par conséquent, en notant $z = a + ib$ avec $a, b \in \mathbb{Z}$, $p = N(z) = a^2 + b^2$, ce qui prouve que $p \in \sum$. □

Théorème 3.

Soit $p \in \mathbb{P}$. Alors, $p \in \sum$ si, et seulement si $p = 2$ ou $p \equiv 1[4]$.

Preuve : Si $p \in \sum$, on a immédiatement $p \not\equiv 0[4]$ (car 4 ne divise pas p). Ensuite, on écrit $p = a^2 + b^2$ avec $a, b \in \mathbb{N}$. Si a est pair, $a^2 \equiv 0[4]$, et si a est impair, $a^2 \equiv 1[4]$. De même pour b, ce qui donne $p \equiv 1[4]$ ou $p \equiv 2[4]$.

Réciproquement, supposons $p = 2$ ou $p \equiv 1[4]$. D'après le lemme précédent, il suffit de montrer que p est réductible dans $\mathbb{Z}[i]$.
Si $p = 2$, alors $p = 1^2 + 1^2$ et donc $p \in \sum$.
Sinon, $p \equiv 1[4]$. Comme $\mathbb{Z}[i]$ est principal (par le lemme 1), il est factoriel. Montrer que p est réductible revient à dire que (p) n'est pas premier, i.e. $\mathbb{Z}[i]/(p)$ n'est pas intègre.
Considérons le morphisme d'évaluation en i $\mathrm{ev}_i : \mathbb{Z}[X] \to \mathbb{Z}[i]$, qui est un morphisme d'anneaux surjectif. On a :

$$\begin{aligned} \mathrm{Ker}(\mathrm{ev}_i) &= \{P \in \mathbb{Z}[X] \mid P(i) = 0\} \\ &= (X^2 + 1), \end{aligned}$$

car le polynôme minimal de i dans $\mathbb{Q}[X]$ est $X^2 + 1$, à coefficients entiers, donc $X^2 + 1$ engendre l'idéal $\mathrm{Ker}(\mathrm{ev}_i)$.
D'après le théorème d'isomorphisme, on a $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2 + 1)$.
En outre, on a, de façon similaire :

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

Maintenant, comme $p \equiv 1[4]$, alors $p - 1 \equiv 0[4]$, donc 2 divise $\dfrac{p-1}{2}$, et $(-1)^{\frac{p-1}{2}} = 1$. -1 est donc un carré modulo p, et $X^2 + 1$ admet alors une racine dans $\mathbb{F}_p$.
Mais alors, $\mathbb{F}_p[X]/(X^2 + 1)$, donc $\mathbb{Z}[i]/(p)$, n'est pas intègre. p n'est donc pas premier dans $\mathbb{Z}[i]$, ce qui prouve que p est réductible dans $\mathbb{Z}[i]$, et cela achève la preuve. □

Corollaire 4.

Soit $n \in \mathbb{N}^*$ avec $n \geqslant 2$. On écrit sa décomposition en facteurs premiers $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$.

Alors, $n \in \sum$ si, et seulement si pour tout entier premier $p \equiv 3[4]$, $v_p(n)$ est pair.

Preuve : Commençons par montrer que $\sum$ est stable par multiplication. Pour $n \in \mathbb{N}$, on a :

$$n \in \sum \iff \exists z \in \mathbb{Z}[i] \quad n = N(z).$$

Soient $n, n' \in \sum$. On écrit $n = N(z)$ et $n' = N(z')$ avec $z, z' \in \mathbb{Z}[i]$. On a alors $nn' = N(zz') \in \sum$, et $\sum$ est stable par multiplication.
Montrons maintenant ce corollaire par double-implication.

$\Longleftarrow$) Soit $n \in \mathbb{N}$ avec $n \geqslant 2$. Supposons que pour tout $p \in \mathbb{P}$ tel que $p \equiv 3[4]$, $v_p(n)$ est pair.
On écrit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}$, avec les p_i et q_i premiers deux à deux distincts, pour tout $(i, j) \in [\![1; r]\!] \times [\![1; s]\!]$, $p_i \equiv 3[4]$ et $q_j \not\equiv 3[4]$, et $\alpha_i, \beta_j \in \mathbb{N}$.
Par hypothèse, les α_i sont pairs. Les $p_i^{\alpha_i}$ s'écrivent alors comme somme de 2 carrés (eux-mêmes et 0), et comme $\sum$ est stable par multiplication, $p_1^{\alpha_1} \cdots p_r^{\alpha_r} \in \sum$.
Ensuite, si $j \in [\![1; s]\!]$, $q_j \not\equiv 3[4]$, et comme q_j est premier, $q_j \not\equiv 0[4]$. Donc $q_j \equiv 1[4]$ ou $q_j \equiv 2[4]$. Dans le dernier cas, 2 divise p_j qui est premier, donc $q_j = 2$.
D'après le lemme précédent, $q_j \in \sum$, donc $q_j^{\beta_j} \in \sum$, et finalement, par stabilité par multiplication de $\sum$, $n \in \sum$.

$\Longrightarrow$) Soit $p \in \mathbb{P}$ tel que $p \equiv 3[4]$. Pour $n \in \mathbb{N}$ avec $n \geqslant 2$, soit $\mathcal{P}(n)$ la propriété : " Si $n \in \sum$, alors $2 | v_p(n)$ ".
Montrons-la par récurrence forte sur $n \geqslant 2$.
Initialisation : Si $n = 2$, on a $n = 1^2 + 1^2 \in \sum$. Comme $p \equiv 3[4]$, p est impair, donc $v_p(n) = 0$, et $2|0 = v_p(n)$. $\mathcal{P}(0)$ est donc vraie.
Hérédité : Soit $n \in \mathbb{N}$ avec $n \geqslant 3$. Supposons $\mathcal{P}(k)$ pour $k \in [\![2; n-1]\!]$. Autrement dit, on suppose que pour tout $k \in [\![2; n-1]\!]$, si $k \in \sum$, alors $2|v_p(k)$.
Supposons $n \in \sum$. Si $v_p(n) = 0$, c'est fini. Sinon, on écrit $n = a^2 + b^2$ avec $a, b \in \mathbb{N}$, et p divise n (dans $\mathbb{Z}$).
Comme $p \equiv 3[4]$, on a $p \notin \sum$ par le théorème précédent, donc par le lemme 2, p est irréductible dans $\mathbb{Z}[i]$.
Maintenant, p divise $n = (a + ib)(a - ib)$ dans $\mathbb{Z}[i]$. D'après le lemme d'Euclide, p divise $a + ib$ ou $a - ib$, dans $\mathbb{Z}[i]$. Sans perte de généralité, on suppose que p divise $a + ib$ dans $\mathbb{Z}[i]$. Comme $p \in \mathbb{Z}$, $p|a$ et $p|b$ (facile à montrer en revenant à la définition de diviser un élément), donc p^2 divise a^2 et b^2, donc p^2 divise n. Autrement dit, $\dfrac{n}{p^2} \in \sum$.
D'après $\mathcal{P}\left(\dfrac{n}{p^2}\right)$, $v_p(n) - 2 = v_p\left(\dfrac{n}{p^2}\right)$ est pair, donc $v_p(n)$ est pair, ce qui achève l'hérédité et la preuve. □