# 1 Développements d'algèbre

## 1.1 Théorème des deux carrés de Fermat

**Théorème.** *Si* $\Sigma = \{a^2 + b^2,\ a, b \in \mathbb{Z}\}$, *alors*

$$n \in \Sigma \iff \forall p \in \mathcal{P},\ p \equiv 3[4],\ v_p(n) \text{ est paire.}$$

— **Lemme.** $\mathbb{Z}[i]$ *est euclidien pour le stathme défini par* $N(z) = |z|^2$.
En effet, si $\alpha, \beta \in \mathbb{Z}[i]$, avec $\beta \neq 0$, soit $z = \alpha/\beta \in \mathbb{C}$. Il existe $\omega \in \mathbb{Z}[i]$ tel que $N(z - \omega) \leq 1/2$ (prendre le point dans $\mathbb{Z}[i]$ le plus proche de $z$, dans le plan complexe). On a $N(\alpha - \beta\omega) \leq N(\beta)/2 < N(\beta)$ donc le quotient $\omega$ convient et $\mathbb{Z}[i]$ est euclidien. Notons que les inversibles sont exactement les éléments de norme unitaire, $\mathbb{Z}[i]^\times = N^{-1}(\{1\}) = \{\pm 1, \pm i\}$. □

— **Lemme.** *Le stathme* $N$ *est multiplicatif, et son image est* $\Sigma$. *Ainsi,* $\Sigma$ *est stable par multiplications.*
Ce résultat trivial cache l'identité de Lagrange : $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.

— **Lemme.** *Si* $p$ *est un nombre premier de* $\mathbb{Z}$, *alors*

$$p \in \Sigma \iff p \text{ est réductible dans } \mathbb{Z}[i] \iff p \not\equiv 3[4].$$

Montrons que les deux premières propositions sont équivalentes, par double implication. En effet, si $p = a^2 + b^2 \in \Sigma$, alors poser $z = a + bi \in \mathbb{Z}[i]$ conduit à $p = z\overline{z}$, et par multiplicativité on a $N(z) = N(\overline{z}) = a^2 + b^2 = p \neq 1$. Ainsi $p$ est produit de deux éléments non-inversible de $\mathbb{Z}[i]$, càd la définition même de réductible. Réciproquement, si $p = zz'$ est réductible avec $z, z' \in \mathbb{Z}[i]$ non-inversible, alors toujours par multiplicativité, $N(p) = p^2 = N(z)N(z')$ donc on a $N(z) = N(z') = p$ (car $N(z)$ et $N(z')$ sont distincts de 1) et ainsi $p$ est somme de deux carrés.
Les deux dernières propositions sont équivalentes, par équivalences directes. En effet, on a $p$ irréductible dans $\mathbb{Z}[i]$ ssi $\mathbb{Z}[i]/(p)$ est intègre. Or, on a les isomorphismes suivants :

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

Cet anneau est intègre ssi $X^2 + 1$ est irréductible sur $\mathbb{F}_p[X]$, càd ssi $-1$ n'est pas un carré dans $\mathbb{F}_p$, càd ssi $p \equiv 3[4]$, en utilisant le symbole de Legendre. Ceci conclut en passant à la négation. □

— **Démonstration du théorème.** On procède par double implication. Commençons par le sens réciproque. Si les valuations $p$-adiques sont paires pour $p \equiv 3[4]$ premier, alors écrivons

$$n = \left( \prod_{p \equiv 3[4]} p^{\frac{v_p(n)}{2}} \right)^2 \prod_{p \not\equiv 3[4]} p^{v_p(n)}.$$

Rappellons que $\Sigma$ est stable par multiplication. Le produit de droite est dans $\Sigma$ car chaque terme l'est (via le troisième lemme). Le produit de gauche aussi, simplement car c'est un carré (et $a^2 = a^2 + 0^2 \in \Sigma$ !). Toujours car $\Sigma$ est stable par multiplication, $n$ est ainsi somme de deux carrés.
Pour le sens direct, procédons par récurrence sur les valuations $p$-adiques, à $p \equiv 3[4]$ fixé :

$$\forall r \in \mathbb{N},\ \forall n \in \Sigma,\ v_p(n) = r \implies v_p(n) \text{ est paire.}$$

C'est clair pour $r = 0$. Supposons le résultat jusqu'à $r$, et soit $n \in \Sigma$ avec $v_p(n) = r + 1$. Si on a $n = a^2 + b^2$, notons $z = a + bi$, de sorte que $n = z\overline{z}$. Comme $v_p(n) \geq 1$, $p$ divise $n = z\overline{z}$, et puisque $p$ est irréductible dans $\mathbb{Z}[i]$ via le lemme, on a $p$ divise $z$ ou $\overline{z}$. Si par exemple, $p$ divise $z$ dans $\mathbb{Z}[i]$, il vient que $p$ divise $a$ et $b$ dans $\mathbb{Z}$, de sorte qu'en factorisant, $n = p^2 m$ où $m \in \Sigma$. Ainsi, $v_p(m) + 2 = v_p(n)$, et $v_p(m) \leq r$, donc $v_p(m)$ puis $v_p(n)$ est paire. □

— **Exemple**. Résoudre $x^2+y^2=mz^2$ tel qu'il existe $p \equiv 3[4]$ tq $v_p(m)$ soit impair. Par exemple, pour les valeurs $m = 3, 6, 7 \ldots$. Il n'y a que la solution triviale !

**Remarques**. Il faut savoir justifier qu'on utilise

$$(A/I)/\pi_I(J) \cong A/(I+J) \cong (A/J)/\pi_J(I).$$

Pour cela, se rappeler qu'une projection d'idéal est bien un idéal, et montrer que si $p$ est la projection de $A/I$ sur $(A/I)/\pi_I(J)$, alors $p \circ \pi_I$ est surjectif de noyau $I+J$, et conclure par premier théorème d'isomorphisme.

Pour la culture, un entier est somme de trois carrés ssi il n'est pas de la forme $4^a(8m+7)$, et tout entier est somme de quatre carrés ! Sinon, dans $\mathbb{F}_q$, tout élément est somme de deux carrés.

Y-a-t'il d'autres irréductibles dans $\mathbb{Z}[i]$ que les $p \equiv 3[4]$ premiers ? Il reste uniquement les $z = a+bi \in \mathbb{Z}[i]$ tq $N(z) = a^2+b^2$ soit premier. En effet, soit $z \in \mathbb{Z}[i]$ irréductible, et soit $p$ premier divisant $N(z) = z\overline{z}$. Soit $p \equiv 3[4]$, donc $p$ est irréductible dans $\mathbb{Z}[i]$ et $p|z$ et $z$ est associé à $p$. Soit $p \not\equiv 3[4]$ et $p = a^2+b^2 \in \Sigma$, et $\omega = a+bi \in \mathbb{Z}[i]$ est irréductible (si $\omega = z_1 z_2$, il vient $p = N(z_1)N(z_2)$ donc $z_1$ ou $z_2$ est associé à $\omega$) et $\omega\overline{\omega}$ divise $z\overline{z}$. Ainsi $\omega$ divise $z$ ou $\overline{z}$, donc $\omega$ est associé à $z$ ou $\overline{z}$.

**Références**. Perrin, Cours d'Algèbre, p. 57, Rombaldi, Algèbre et géométrie, p. 267.