Théorème des deux carrés

Référence : Perrin : Cours d'algèbre p.56,57,58 ou Risler-Boyer : Algèbre pour le L3 Problème 1.4 p23+159 + Gourdon Algèbre

Soit $\Sigma = \{n \in \mathbb{N} \mid n = a^2 + b^2;\ a, b \in \mathbb{N}\}$.

Théorème (des deux carrés)

Soit p un nombre premier impair [1].
On a l'équivalence suivante :

$$p \in \Sigma \Longleftrightarrow p \equiv 1\ [4]$$

Pour démontrer ce théorème, l'idée est de penser que si $n \in \Sigma$, alors $n = a^2 + b^2 = (a + \mathrm{i}b)(a - \mathrm{i}b)$ dans $\mathbb{C}$. On va donc introduire l'anneau des entiers de Gauss $\mathbb{Z}[\mathrm{i}]$.

1 L'anneau $\mathbb{Z}[\mathrm{i}]$

Définition

On définit l'anneau $\mathbb{Z}[\mathrm{i}]$ comme le plus petit sous-anneau de $\mathbb{C}$ contenant $\mathbb{Z}$ et i. On montre, en utilisant le fait que $\mathrm{i}^2 = -1$ que :

$$\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b \in \mathbb{C} | a, b \in \mathbb{Z}\}$$

Cet anneau est intègre car inclus dans $\mathbb{C}$. De plus, on dispose d'un automorphisme de $\mathbb{Z}[\mathrm{i}]$ donné par la conjugaison :

$$\begin{array}{rccc} \sigma\ : & \mathbb{Z}[\mathrm{i}] & \to & \mathbb{Z}[\mathrm{i}] \\ z = a + \mathrm{i}b & \mapsto & \bar{z} = a - \mathrm{i}b \end{array}$$

Cet automorphisme nous permet de définir une "norme"

$$\begin{array}{rccc} N\ : & \mathbb{Z}[\mathrm{i}] & \to & \mathbb{N} \\ a + \mathrm{i}b & \mapsto & z\bar{z} = a^2 + b^2 \end{array}$$

qui est multiplicative, c'est à dire $N(zz') = N(z)N(z')$.
L'introduction de cette norme permet de calculer les inversibles de $\mathbb{Z}[\mathrm{i}]$:

Proposition 1

On a $\mathbb{Z}[\mathrm{i}]^* = \{\pm 1, \pm \mathrm{i}\}$.

Preuve :
Si $z \in \mathbb{Z}[\mathrm{i}]^*$, $\exists z' \in \mathbb{Z}[\mathrm{i}]^*$ tel que $zz' = 1$, d'où $N(z)N(z') = 1$.
Donc $N(z) = N(z') = 1 \ \Rightarrow\ a^2 + b^2 = 1 \ \Rightarrow\ (a = 0 \text{ et } b = \pm 1)$ ou $(a = \pm 1 \text{ et } b = 0)$.
D'où le résultat. ■

Proposition 2

L'ensemble Σ des sommes de deux carrés est stable par multiplication.

1. Il est clair que $2 \in \Sigma$ car $2 = 1^2 + 1^2$ mais $2 \not\equiv 1\ [4]$.

Preuve :
On traduit la propriété $n \in \Sigma$ en termes d'entiers de Gauss :

$$n \in \Sigma \Leftrightarrow \exists z \in \mathbb{Z}[\mathrm{i}] \ / \ n = N(z)$$

Alors, si $n, n' \in \Sigma$, on a $n = N(z)$ et $n' = N(z')$ donc $nn' = N(zz') \in \Sigma$ ■

Proposition 3

L'anneau $\mathbb{Z}[\mathrm{i}]$ est euclidien pour le stathme N, donc principal.

Preuve :
Soient $z, t \in \mathbb{Z}[\mathrm{i}]\backslash\{0\}$. On a $z/t \in \mathbb{C}$ qui est de la forme $z/t = x + \mathrm{i}y$.
On veut approximer $\dfrac{z}{t}$ par un entier de Gauss $q = a + \mathrm{i}b$ où a et b sont les plus proches entiers de x et y respectivement donc $|x - a| \leqslant \dfrac{1}{2}$ et $|y - b| \leqslant \dfrac{1}{2}$. Ainsi,

$$\left|\frac{z}{t} - q\right| \leqslant \frac{\sqrt{2}}{2} < 1$$

On pose alors $r = z - qt$ et ainsi $r \in \mathbb{Z}[\mathrm{i}]$ (car z, q et t le sont) et $r = t\left(\dfrac{z}{t} - q\right)$ d'où

$$|r| = |t| \ \left|\frac{z}{t} - q\right| < |t| \ \text{ et en élevant au carré, } \ N(r) < N(t).$$

On a donc bien écrit $z = qt + r$ avec $N(r) < N(t)$ et le résultat est démontré. ■

2 Démonstration du théorème des deux carrés

On rappelle le théorème à démontrer :

Théorème

Soit p un nombre premier impair.
On a l'équivalence suivante :

$$p \in \Sigma \Longleftrightarrow p \equiv 1 \ [4]$$

Remarquons déjà (ce sera redémontré dans la suite) que la condition $p \equiv 1$ [4] est clairement nécessaire car $\forall (a, b) \in \mathbb{N}^2$, $a^2 + b^2 \equiv 0, 1, 2$ [4] et comme p est premier, $p \not\equiv 0$ ou 2 [4].

Lemme

On a l'équivalence suivante :

$$p \in \Sigma \iff p \text{ n'est pas irréductible dans } \mathbb{Z}[\mathrm{i}].$$

Preuve du Lemme :

($\Rightarrow$) : Si $p = a^2 + b^2$, on a $p = (a + \mathrm{i}b)(a - \mathrm{i}b)$ et a, b sont $\neq 0$, donc $a + \mathrm{i}b$, $a - \mathrm{i}b$ ne sont pas dans $\mathbb{Z}[\mathrm{i}]^*$ d'où p n'est pas irréductible.
($\Leftarrow$) : Si $p = zz'$ avec z, z' non inversibles (donc $N(z), N(z')$ sont $\neq 1$), on a $N(p) = N(z)N(z') = p^2$, donc comme p est premier, nécessairement $p = N(z)$ d'où $p \in \Sigma$ et le lemme est démontré. ■

Preuve du Théorème :

$\mathbb{Z}[\mathrm{i}]$ est factoriel (car euclidien pour le stathme N).
On a donc l'équivalence suivante :

$$\begin{array}{lcl} p \text{ n'est pas irréductible dans } \mathbb{Z}[\mathrm{i}] & \underset{\text{Lemme d'Euclide}}{\Longleftrightarrow} & (p) \text{ n'est pas premier dans } \mathbb{Z}[\mathrm{i}] \\ & \Longleftrightarrow & \mathbb{Z}[\mathrm{i}]/(p) \text{ non intègre.} \end{array}$$

De plus, $\mathbb{Z}[\mathrm{i}] \simeq \mathbb{Z}[X]/(X^2+1)$ donc on a [2] :

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

D'où,

$$\begin{array}{rcl} p \text{ est réductible dans } \mathbb{Z}[\mathrm{i}] & \iff & p \text{ n'est pas irréductible dans } \mathbb{Z}[\mathrm{i}] \\ & \iff & X^2+1 \text{ n'est pas irréductible dans } \mathbb{F}_p[X] \\ & \underset{\text{car } X^2+1 \text{ est de deg 2}}{\iff} & X^2+1 \text{ admet une racine dans } \mathbb{F}_p \\ & \iff & -1 \text{ est un carré dans } \mathbb{F}_p. \end{array}$$

D'après le lemme, il nous reste donc juste à démontrer que :

$$-1 \text{ est un carré dans } \mathbb{F}_p \iff p \equiv 1\ [4]$$

Pour démontrer cela, soit on fait comme dans Gourdon p.37 ce qui nous passe du symbole de Legendre.
Soit : si p impair, on a

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si} \quad p \equiv 1\ [4] \\ -1 & \text{sinon} \end{cases}$$

Et finalement, le théorème est démontré. ■

Corollaire

Soit $n \in \mathbb{N}^*$. On décompose n en produit de facteurs premiers : $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$ où $\mathcal{P} = \{\text{nombres premiers}\}$.
Alors,

$$n \in \Sigma \iff \forall p \in \mathcal{P} \text{ tel que } p \equiv 3\ [4], \quad \nu_p(n) \text{ est pair.}$$

Preuve :

($\Leftarrow$) : On décompose n de la façon suivante car lorsque $p \equiv 3\ [4]$, $\nu_p(n)$ est pair :

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

Le produit de gauche est un carré parfait donc il appartient à Σ.
Dans le produit de droite, chaque p est congru à 1 modulo 4 ou égal à 2 donc dans Σ.
La stabilité par multiplication de Σ permet alors de conclure.

($\Rightarrow$) : (Gourdon p.49) On a $n = a^2 + b^2$. Soit $d = \mathrm{pgcd}(a,b)$.
Les nombres $A = \frac{a}{d}$ et $B = \frac{b}{d}$ sont premiers entre eux. De plus $n = d^2(A^2+B^2)$.
Soit $p \in \mathcal{P}$ tel que p divise n tel que l'exposant de p dans la décomposition en facteur premier de n est impair. Du coup, p divise A^2+B^2. Or p ne divise pas A. En effet, si p divisait A, alors p diviserait B ce qui est exclu car A et B sont premiers entre eux.
Ainsi $\bar{A}$ non nul dans $\mathbb{F}_p^*$. Et comme $\bar{A}^2 + \bar{B}^2 = 0$ et $(\overline{A^{-1}B})^2 = -1$,c'est-à-dire -1 est un carré modulo p ie cela entraîne que $p = 2$ ou $p \equiv 1\ [4]$. Donc tous les gens premiers $\equiv 3\ [4]$ ont bien leur valuation paire (sorte d'absurde ici).

■

2. Il faut savoir expliciter ces isomorphismes. Pour cela considérer les projections canoniques et faire du thm d'isomorphisme en considérant le Ker des composées. Ce sera surement bien fait sur la page de Flo cet été.

Notes :

✓ **A l'oral**,11'11 en très vite. Il faut faire une intro sur $\mathbb{Z}[i]$ avec inversibles et stable par multiplication. Puis corollaire, puis thm pour p premier.
✓ On peut prendre la fin du corollaire dans Duverney.
♣ Carl Gauss (1777 - 1855) est un mathématicien, astronome et physicien allemand. Il a apporté de très importantes contributions à ces trois domaines. Surnommé "le prince des mathématiciens" (Mathematicorum Principi), il est considéré comme l'un des plus grands mathématiciens de tous les temps. La qualité extraordinaire de ses travaux scientifiques était déjà reconnue par ses contemporains. Il dirigea l'Observatoire de Göttingen et ne travailla pas comme professeur de mathématiques – d'ailleurs il n'aimait guère enseigner – mais il encouragea plusieurs de ses étudiants, qui devinrent d'importants mathématiciens, notamment Eisenstein et Riemann. Il a beaucoup échangé avec Sophie Germain et était assez fan d'elle (un féministe !).