

Feuille d'exercices numéro 7 : le théorème des deux carrés

Dans cet exercice, on montre le théorème des deux carrés, qui caractérise les entiers naturels qui sont sommes de deux carrés d'entiers. C'est un grand classique. On note $\mathcal{P}$ l'ensemble des nombres premiers.

Théorème 1 (théorème des deux carrés)

Soit n un entier naturel non nul, et $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ sa décomposition en produit de nombres premiers. Alors, n est la somme de deux carrés d'entiers si, et seulement si

$$\forall p \in \mathcal{P}, p \equiv 3 \pmod{4} \implies v_p(n) \text{ est pair.}$$

Commencer par contempler ce résultat en le confrontant aux premiers entiers.

Préliminaire Montrer l'identité polynomiale dans $\mathbb{Z}[X, Y, Z, T]$

$$(X^2 + Y^2)(Z^2 + T^2) = (XZ - YT)^2 + (XT + YZ)^2. \quad (1)$$

En donner une interprétation (et une preuve sans calcul) en termes de nombres complexes.

En déduire que l'ensemble des sommes de deux carrés d'entiers est stable pour la multiplication.

1 L'anneau des entiers de Gauss

Soit $\mathbb{Z}[i]$ le sous-anneau de $\mathbb{C}$ engendré par i . On l'appelle anneau des *entiers de Gauss*. Si $a, b \in \mathbb{Z}$, on note $N(a + ib) = a^2 + b^2$ la *norme*[♠] de l'entier de Gauss $a + ib$.

1.1) Vérifier que $N(xy) = N(x)N(y)$ pour tous $x, y \in \mathbb{Z}[i]$. Calculer tous les inversibles de $\mathbb{Z}[i]$.

1.2) Montrer que pour tout $x \in \mathbb{Z}[i]$, pour tout $d \in \mathbb{Z}[i] \setminus \{0\}$, il existe $q, r \in \mathbb{Z}[i]$ tels que $x = dq + r$ avec $N(r) \leq N(d) - 1$ (dans le jargon, on dit que l'anneau $\mathbb{Z}[i]$ est *euclidien* pour N).

[Indication : approcher le nombre complexe x/d par un entier de Gauss approprié (faire un dessin).]

1.3) Soit p un nombre premier. Montrer que p est somme de deux carrés d'entiers si, et seulement si p est réductible dans $\mathbb{Z}[i]$.

1.4) Soit p un nombre premier. Montrer que

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

et que cet anneau est intègre si, et seulement si -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$. En déduire que p est réductible dans $\mathbb{Z}[i]$ si, et seulement si -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

2 Application au théorème des deux carrés

2.1) Soit p un nombre premier impair. Montrer que $p \equiv 1 \pmod{4}$ si, et seulement si $(-1)^{\frac{p-1}{2}} = 1$.

2.2) Soit p un nombre premier, $p \geq 3$. Montrer que le nombre de carrés non nuls dans $\mathbb{Z}/p\mathbb{Z}$ est $\frac{p-1}{2}$.

[Indication : on pourra considérer l'application $x \mapsto x^2$ dans ce corps.]

[♠]Attention, cela n'est pas une norme au sens des espaces vectoriels normés ; ce vocabulaire est emprunté à la théorie algébrique des nombres.

2.3) Soit p un nombre premier différent de 2. Montrer que l'ensemble des carrés non nuls de $\mathbb{Z}/p\mathbb{Z}$ est l'ensemble de ses éléments x qui vérifient $x^{\frac{p-1}{2}} = 1$.

[Indication : on pourra considérer l'application $x \mapsto x^{\frac{p-1}{2}}$.]

2.4) Soit p un nombre premier. Montrer que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si $p = 2$ ou $p \equiv 1 \pmod{4}$.

2.5) Soit p un nombre premier. Montrer que p est somme de deux carrés d'entiers si, et seulement si $p = 2$ ou $p \equiv 1 \pmod{4}$.

2.6) Prouver le théorème 1 (on pourra faire une récurrence pour le sens direct).

2.7) Retour aux entiers de Gauss : caractériser les irréductibles de $\mathbb{Z}[i]$.