DM 10 : théorèmes des deux et des quatre carrés [corrigé]

Partie I. Arithmétique dans $\mathbb{Z}[i]$.

- On considère l'ensemble $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$.
- On note N l'application *norme*[1]

$$N : \begin{cases} \mathbb{Z}[i] \to \mathbb{R} \\ \alpha \mapsto |\alpha|^2 \end{cases}.$$

- Soit $\alpha, \beta \in \mathbb{Z}[i]$. On dit que α *divise* β *(dans* $\mathbb{Z}[i]$*)* s'il existe $\kappa \in \mathbb{Z}[i]$ tel que $\beta = \kappa\,\alpha$.

1. Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.

   - *On a clairement* $1 = 1 + i \times 0 \in \mathbb{Z}[i]$.
   - *Soit* $\alpha_1, \alpha_2 \in \mathbb{Z}[i]$. *On peut donc trouver* $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ *tels que* $\alpha_1 = x_1 + iy_1$ *et* $\alpha_2 = x_2 + iy_2$.
     - *On a* $\alpha_1 - \alpha_2 = (x_1 - x_2) + i(y_1 - y_2) \in \mathbb{Z}[i]$.
     - *On a* $\alpha_1\,\alpha_2 = (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1) \in \mathbb{Z}[i]$.

   L'ensemble $\mathbb{Z}[i]$ *contient* 1*, et est stable par différence et produit, donc il s'agit d'un sous-anneau de* $\mathbb{C}$.

2. (a) Montrer que le groupe additif $\mathbb{Z}[i]$ est engendré par la famille $(1, i)$.

   - *L'inclusion* $\langle 1, i\rangle \subseteq \mathbb{Z}[i]$ *est automatique.*
   - *Soit* $\alpha \in \mathbb{Z}[i]$. *On peut donc trouver* $x, y \in \mathbb{Z}$ *tels que* $\alpha = x + iy$.
     - *Comme le sous-groupe* $\langle 1, i\rangle$ *contient* 1*, il contient* $x\,1 = x$ *(stabilité par « puissances » additives).*
     - *Comme le sous-groupe* $\langle 1, i\rangle$ *contient* i*, il contient* yi.

     Par stabilité par somme, on a donc $\alpha \in \langle 1, i\rangle$*, ce qui montre* $\mathbb{Z}[i] \subseteq \langle 1, i\rangle$*, et conclut.*

   (b) Soit $\varphi : \mathbb{Z}[i] \to \mathbb{Z}[i]$ un endomorphisme d'anneaux. Montrer que $\varphi(i) = \pm i$.

   Comme φ *est un morphisme d'anneaux, on a* $\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -\varphi(1) = -1$*, ce qui montre* $\varphi(i) = \pm i$.

   (c) En déduire que $\mathbb{Z}[i]$ possède exactement deux endomorphismes d'anneaux, et que les deux sont des automorphismes.

   - *Il est déjà clair que* $\mathrm{id}_{\mathbb{Z}[i]}$ *et la conjugaison complexe (induite)* $C : \begin{cases} \mathbb{Z}[i] & \to & \mathbb{Z}[i] \\ \alpha = x + iy & \mapsto & \overline{\alpha} = x - iy \end{cases}$ *sont deux automorphismes de* $\mathbb{Z}[i]$.
   - *Soit maintenant* $\varphi : \mathbb{Z}[i] \to \mathbb{Z}[i]$ *un endomorphisme d'anneaux. On va montrer que* φ *est l'un des deux automorphismes que l'on vient de citer.*
     - *Comme* φ *est un endomorphisme d'anneaux, on a* $\varphi(1) = 1$.
     - *D'après la question précédente, on a* $\varphi(i) = \pm i$.

1. Géométriquement, il s'agit plutôt du carré de la norme, mais le mot « norme » est standard en arithmétique.

Ainsi, φ (qui est en particulier un morphisme de groupes additifs) coïncide avec $\mathrm{id}_{\mathbb{Z}[i]}$ ou la conjugaison complexe sur la famille $(1, i)$.
D'après la question précédente et le théorème de prolongement des identités, on a donc $\varphi = \mathrm{id}_{\mathbb{Z}[i]}$ ou $\varphi = C$.

3. Montrer que l'application N est à valeurs dans $\mathbb{N}$ et qu'elle est *multiplicative*, c'est-à-dire que

$$\forall \alpha, \beta \in \mathbb{Z}[i], N(\alpha\,\beta) = N(\alpha)\,N(\beta).$$

► *Soit $\alpha \in \mathbb{Z}[i]$. On peut donc trouver $x, y \in \mathbb{Z}$ tels que $\alpha = x + iy$. On a alors*

$$N(\alpha) = x^2 + y^2 \in \mathbb{N}.$$

► *La multiplicativité de N découle directement de celle du module.*

4. Montrer que $\mathbb{Z}[i]^\times = \left\{\alpha \in \mathbb{Z}[i] \,\middle|\, N(\alpha) = 1\right\}$ et en déduire que $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

► • *Soit $\alpha \in \mathbb{Z}[i]^\times$. On a alors $\alpha\,\alpha^{-1} = 1$. En passant à la norme, il vient*

$$\underbrace{N(\alpha)}_{\in\mathbb{N}}\,\underbrace{N\left(\alpha^{-1}\right)}_{\in\mathbb{N}} = 1.$$

$N(\alpha)$ est donc un entier naturel dont l'inverse est encore un entier naturel, d'où $N(\alpha) = 1$.

• *Réciproquement, soit $\alpha \in \mathbb{Z}[i]$ tel que $N(\alpha) = 1$. On a donc $1 = |\alpha|^2 = \alpha\,\overline{\alpha}$. Comme $\mathbb{Z}[i]$ est clairement stable par conjugaison, on a $\overline{\alpha} \in \mathbb{Z}[i]$ et donc $\alpha \in \mathbb{Z}[i]$ (d'inverse $\overline{\alpha}$).*

► • *Soit $\alpha \in \mathbb{Z}[i]$ tel que $N(\alpha) = 1$.*
On peut donc trouver $x, y \in \mathbb{Z}$ tels que $\alpha = x + iy$ et donc $N(\alpha) = x^2 + y^2 = 1$.
Cela entraîne que $(x^2, y^2) = (1, 0)$ ou $(x^2, y^2) = (0, 1)$, d'où l'on tire $\alpha \in \{\pm 1, \pm i\}$.

• *Réciproquement, l'inclusion $\{\pm 1, \pm i\} \subseteq \left\{\alpha \in \mathbb{Z}[i] \,\middle|\, N(\alpha) = 1\right\}$ est claire.*

5. Soit $a, b, c \in \mathbb{Z}$, et $\alpha = a + ib$.
   (a) Montrer que c divise α (dans $\mathbb{Z}[i]$) si et seulement si c divise a et b (dans $\mathbb{Z}$).

On a la chaîne d'équivalences

$$\begin{aligned} c \textit{ divise } \alpha \textit{ dans } \mathbb{Z}[i] &\Leftrightarrow \exists \kappa \in \mathbb{Z}[i] : \alpha = \kappa c \\ &\Leftrightarrow \exists x, y \in \mathbb{Z} : a + ib = (x + iy)c \\ &\Leftrightarrow \exists x, y \in \mathbb{Z} : \begin{cases} a = xc \\ b = yc \end{cases} \\ &\Leftrightarrow c \textit{ divise } a \textit{ et } b \textit{ dans } \mathbb{Z}. \end{aligned}$$

   (b) En déduire que c divise a dans $\mathbb{Z}[i]$ si et seulement si c divise a dans $\mathbb{Z}$.

Il suffit d'appliquer la question précédente à $b = 0$.

► La dernière question levant toute ambiguïté, on notera simplement | la relation de divisibilité : étant donné $\alpha, \beta \in \mathbb{Z}[i]$, on notera $\alpha \mid \beta$ si $\exists \kappa \in \mathbb{Z}[i] : \beta = \kappa\,\alpha$.

6. Soit $\alpha, \beta \in \mathbb{Z}[i]$. Montrer l'équivalence $\big(\alpha \mid \beta \text{ et } \beta \mid \alpha\big) \Leftrightarrow \exists \varepsilon \in \mathbb{Z}[i]^\times : \beta = \varepsilon\,\alpha$.

   - *Supposons $\alpha \mid \beta$ et $\beta \mid \alpha$: on peut donc trouver $\kappa, \lambda \in \mathbb{Z}[i]$ tels que $\beta = \kappa\,\alpha$ et $\alpha = \lambda\,\beta$.*
     On a donc $\beta = (\kappa\lambda)\,\beta$.
     - *Si $\beta = 0$, on a nécessairement $\alpha = 0$, et il s'ensuit $\exists \varepsilon \in \mathbb{Z}[i]^\times : \beta = \varepsilon\,\alpha$ (car $\varepsilon = 1$ convient).*
     - *Sinon, l'égalité précédente montre que $\kappa\lambda = 1$, donc $\kappa, \lambda \in \mathbb{Z}[i]^\times$ et $\varepsilon = \kappa$ convient.*
   - *Réciproquement, si l'on peut trouver $\varepsilon \in \mathbb{Z}[i]^\times$ tel que $\beta = \varepsilon\,\alpha$, on a clairement $\alpha \mid \beta$ et l'égalité $\alpha = \varepsilon^{-1}\alpha$ donne également $\beta \mid \alpha$.*

- Comme dans le cas de $\mathbb{Z}$, on dira que α et $\beta \in \mathbb{Z}[i]$ sont *associés* si $\exists \varepsilon \in \mathbb{Z}[i]^\times : \beta = \varepsilon\alpha$.
- Un élément $\pi \in \mathbb{Z}[i]$ est dit *irréductible* si $\pi \neq 0$, $\pi \notin \mathbb{Z}[i]^\times$, et que

$$\forall \alpha, \beta \in \mathbb{Z}[i], \pi = \alpha\,\beta \Rightarrow \big(\alpha \in \mathbb{Z}[i]^\times \text{ ou } \beta \in \mathbb{Z}[i]^\times\big)\,.$$

7. Soit $\pi \in \mathbb{Z}[i]$ tel que $N(\pi)$ soit un nombre premier. Montrer que π est irréductible.

   - *Déjà, $N(\pi) \notin \{0, 1\}$, donc π n'est ni nul, ni inversible.*
   - *Soit maintenant $\alpha, \beta \in \mathbb{Z}[i]$ tels que $\pi = \alpha\beta$.*
     Par multiplicativité de la norme, on a $N(\pi) = N(\alpha)\,N(\beta)$.
     Comme $N(\pi)$ est premier, on a $N(\alpha) = 1$ (auquel cas, $\alpha \in \mathbb{Z}[i]^\times$) ou $N(\beta) = 1$ (auquel cas, $\beta \in \mathbb{Z}[i]$), ce qui conclut.

8. **Exemples.** Un nombre premier p est un élément de $\mathbb{Z}[i]$, mais rien ne dit qu'il soit irréductible. Dans cette question, on constate que les trois premiers nombres premiers ont des destins différents.

   (a) 2 **est « ramifié ».** Montrer que 2 n'est pas irréductible dans $\mathbb{Z}[i]$.
   Plus précisément, trouver $\pi \in \mathbb{Z}[i]$ irréductible tel que 2 soit associé à π^2.

   On a $2 = -i(1+i)^2$, donc 2 est associé à $(1+i)^2$.
   La question précédente montre directement que $1+i$, de norme 2, est irréductible.

   (b) 3 **est « inerte ».** Montrer que 3 n'est pas la somme de deux carrés parfaits et en déduire que 3 est irréductible dans $\mathbb{Z}[i]$.

   - *Les seuls carrés parfaits $\leqslant 3$ sont 0 et 1. Comme un carré parfait est nécessairement positif et que la somme de deux éléments de $\{0, 1\}$ ne peut jamais valoir 3, on en déduit que 3 n'est pas la somme de deux carrés parfaits.*
   - *Montrons maintenant que 3 est irréductible.*
     - *Comme $N(3) = 9 > 1$, 3 n'est ni nul, ni inversible.*
     - *Soit $\alpha, \beta \in \mathbb{Z}[i]$ tels que $3 = \alpha\,\beta$. Par multiplicativité de la norme, on en déduit*

$$N(3) = 9 = N(\alpha)\,N(\beta),$$

     ce qui montre déjà que $N(\alpha), N(\beta) \in \{1, 3, 9\}$.

     ▷ *Comme $N(\alpha) = (\text{Ré}\,\alpha)^2 + (\text{Im}\,\alpha)^2$, il s'agit de la somme de deux carrés parfaits, et on a donc $N(\alpha) \neq 3$.*

     ▷ *Si $N(\alpha) = 1$, on a $\alpha \in \mathbb{Z}[i]^\times$.*

     ▷ *Si $N(\alpha) = 9$, on a $N(\beta) = 1$ et $\beta \in \mathbb{Z}[i]^\times$.*

     Cela conclut.

(c) 5 **est « totalement décomposé ».** Montrer que 5 n'est pas irréductible dans $\mathbb{Z}[i]$.
Plus précisément, trouver $\pi_1, \pi_2 \in \mathbb{Z}[i]$ irréductibles et non associés tels que $5 = \pi_1 \pi_2$.

On a $5 = (2+i)(2-i)$.
Comme $N(2+i) = N(2-i) = 5$, *ces deux éléments sont irréductibles.*
Enfin, $2+i$ *et* $2-i$ *ne sont pas associés : s'ils l'étaient, on pourrait trouver* $\varepsilon \in \mathbb{Z}[i]$ *tel que* $2+i = \varepsilon(2-i)$, *ce qui entraînerait* $\varepsilon = \dfrac{2+i}{2-i} = \dfrac{3}{5} + i\dfrac{4}{5}$. *C'est une contradiction, car cet élément n'appartient pas à* $\mathbb{Z}[i]$.

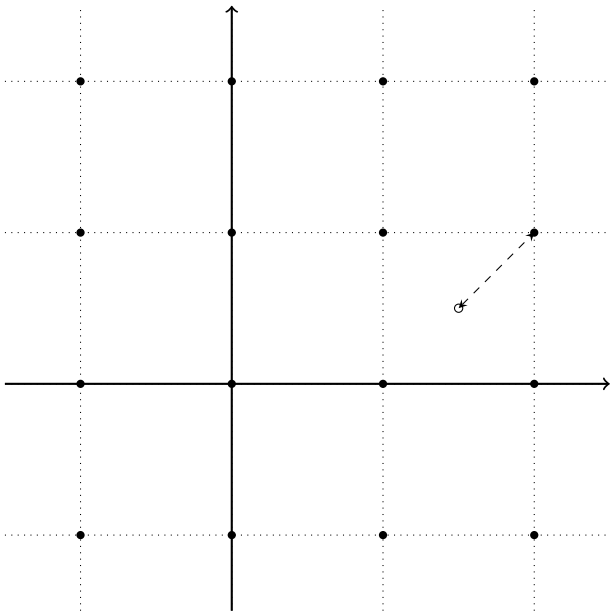
9. **Division euclidienne dans** $\mathbb{Z}[i]$**.**
(a) Montrer que $\forall z \in \mathbb{C}, \exists \kappa \in \mathbb{Z}[i] : |z - \kappa| < 1$.

Soit $z = x + iy \in \mathbb{C}$.

- *En prenant l'entier le plus proche, on peut trouver* $a, b \in \mathbb{Z}$ *tels que* $|x - a| \leqslant \dfrac{1}{2}$ *et* $|y - b| \leqslant \dfrac{1}{2}$.
On a alors $\kappa = a + ib \in \mathbb{Z}[i]$ *et*

$$\left|(x+iy) - (a+ib)\right|^2 = (x-a)^2 + (y-b)^2 \leqslant \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 \leqslant \frac{1}{2},$$

donc $|z - \kappa| \leqslant \dfrac{1}{\sqrt{2}} < 1$.



Tout point de $\mathbb{C}$ *est à distance* $\leqslant \dfrac{1}{\sqrt{2}}$ *d'un point de* $\mathbb{Z}[i]$.

(b) En déduire que pour tous $\alpha, \beta \in \mathbb{Z}[i]$ tels que $\beta \neq 0$, il existe $\kappa, \rho \in \mathbb{Z}[i]$ tels que

$$\alpha = \kappa\,\beta + \rho \qquad \text{et} \qquad N(\rho) < N(\beta).$$

Soit $\alpha, \beta \in \mathbb{Z}[i]$ *tels que* $\beta \neq 0$. *Posons* $z = \dfrac{\alpha}{\beta} \in \mathbb{C}$.
D'après la question précédente, on peut trouver $\kappa \in \mathbb{Z}[i]$ *tel que* $|z - \kappa| < 1$. *Par stricte croissance de* $t \mapsto t^2$ *sur* $\mathbb{R}_+$, *on a même* $\left|\dfrac{\alpha}{\beta} - \kappa\right|^2 = |z - \kappa|^2 < 1$.
Ainsi,

$$N(\alpha - \kappa\,\beta) = |\alpha - \kappa\,\beta|^2 = \left|\frac{\alpha}{\beta} - \kappa\right|^2 |\beta|^2 < |\beta|^2 = N(\beta),$$

ce qui conclut (en posant $\rho = \alpha - \kappa\,\beta$, *ce qui rend l'égalité* $\alpha = \kappa\,\beta + \rho$ *tautologique).*

10. **Un théorème de Bézout.** Soit $\alpha, \beta \in \mathbb{Z}[i]$ non tous les deux nuls. On définit

$$(\alpha, \beta) = \left\{ \lambda\,\alpha + \mu\,\beta \,\middle|\, \lambda, \mu \in \mathbb{Z}[i] \right\}.$$

Par ailleurs, pour tout $\gamma \in \mathbb{Z}[i]$, on définit $(\gamma) = \left\{ \nu\,\gamma \,\middle|\, \nu \in \mathbb{Z}[i] \right\}$.
Montrer qu'il existe $\delta \in \mathbb{Z}[i]$ tel que $(\alpha, \beta) = (\delta)$.

Conformément à l'indication, remarquons que (α, β) n'est pas réduit à $\{0\}$ (car il contient α et β, qui ne sont pas tous les deux nuls). On peut donc trouver $\delta \in (\alpha, \beta)$ de norme minimale parmi les éléments non nuls de (α, β). (Plus formellement, $\{N(\gamma) \,|\, \gamma \in (\alpha, \beta) \setminus \{0\}\}$ est une partie non vide de $\mathbb{N}$, donc elle admet un minimum, et on peut trouver $\delta \in (\alpha, \beta) \setminus \{0\}$ tel que $N(\delta)$ soit ce minimum).
Montrons maintenant $(\delta) = (\alpha, \beta)$.

- *Soit $\zeta \in (\delta)$. On peut donc trouver $\nu \in \mathbb{Z}[i]$ tel que $\zeta = \nu\,\delta$.*
  Comme $\delta \in (\alpha, \beta)$, on peut trouver $\lambda, \mu \in \mathbb{Z}[i]$ tels que $\delta = \lambda\,\alpha + \mu\,\beta$.
  On obtient ainsi

$$\zeta = \nu\,\delta = (\nu\,\lambda)\alpha + (\nu\,\mu)\beta \in (\alpha, \beta).$$

- *Réciproquement, soit $\zeta \in (\alpha, \beta)$.*
  Grâce à la question précédente, on peut trouver $\kappa, \rho \in \mathbb{Z}[i]$ tels que

$$\zeta = \kappa\,\delta + \rho \qquad \text{et} \qquad N(\rho) < N(\delta).$$

  En particulier, $\rho = \zeta - \kappa\,\delta$.
  - *Par hypothèse, $\zeta \in (\alpha, \beta)$.*
  - *Le point précédent de la démonstration montre que $(\delta) \subseteq (\alpha, \beta)$, donc $\kappa\,\delta \in (\alpha, \beta)$.*
  - *On voit directement que (α, β) est stable par différence (c'est même un sous-groupe additif de $\mathbb{Z}[i]$, mais peu importe).*

  Ainsi, on a $\rho \in (\alpha, \beta)$.
  Comme $N(\rho) < N(\delta)$ et que $N(\delta)$ est, par définition, la norme minimale d'un élément non nul de (α, β), on a nécessairement $N(\rho) = 0$, donc $\rho = 0$, donc $\zeta = \kappa\,\delta$.
  Cela montre $\zeta \in (\delta)$, et conclut.

11. **Un lemme d'Euclide.** Soit $\pi \in \mathbb{Z}[i]$ irréductible.
    (a) Montrer que pour tout $\alpha \in \mathbb{Z}[i]$ tel que $\pi \nmid \alpha$, il existe $\lambda, \mu \in \mathbb{Z}[i]$ tel que $\lambda\,\alpha + \mu\,\pi = 1$.

    D'après la question précédente, on peut trouver $\delta \in \mathbb{Z}[i]$ tel que $(\alpha, \pi) = (\delta)$.
    En particulier, on a $\pi \in (\delta)$, donc on peut trouver $\kappa \in \mathbb{Z}[i]$ tel que $\pi = \kappa\,\delta$.
    Par irréductibilité de π, il y a deux possibilités :
    - *Si κ est inversible, on obtient $\delta = \kappa^{-1}\,\pi$. Puisque $\alpha \in (\delta)$, on peut trouver $\lambda \in \mathbb{Z}[i]$ tel que $\alpha = \lambda\,\delta = \lambda\,\kappa^{-1}\,\pi$, ce qui contredit l'hypothèse $\pi \nmid \alpha$. Ce cas est donc impossible.*
    - *Si δ est inversible, on a $1 = \delta^{-1}\,\delta \in (\delta) = (\alpha, \beta)$, ce qui donne l'existence de $\lambda, \mu \in \mathbb{Z}[i]$ tels que $1 = \lambda\,\alpha + \mu\,\pi$, et conclut.*

    (b) Soit $\alpha_1, \ldots, \alpha_r \in \mathbb{Z}[i]$. Montrer $\pi \mid \alpha_1 \cdots \alpha_r \Leftrightarrow \exists j \in [\![1, r]\!] : \pi \mid \alpha_j$.

    - • *Montrons d'abord l'implication directe dans le cas $r = 2$.*
      Supposons $\pi \mid \alpha_1\,\alpha_2$. On peut donc trouver $\kappa \in \mathbb{Z}[i]$ tel que $\alpha_1\,\alpha_2 = \kappa\,\pi$.
      On va montrer $\pi \nmid \alpha_1 \Rightarrow \pi \mid \alpha_2$.
      Supposons $\pi \nmid \alpha_1$.
      D'après la question précédente, on peut trouver $\lambda, \mu \in \mathbb{Z}[i]$ tels que $\lambda\,\alpha_1 + \mu\,\pi = 1$. On a donc

$$\alpha_2 = \lambda\,\alpha_1\,\alpha_2 + \mu\,\pi\,\alpha_2 = (\lambda\,\kappa + \mu\,\alpha_2)\,\pi,$$

      ce qui montre $\pi \mid \alpha_2$, et conclut.

- *En appliquant le cas* $r = 2$*, on obtient que* $\pi \mid \alpha_1(\alpha_2 \cdots \alpha_r) \Rightarrow \pi \mid \alpha_1$ *ou* $\pi \mid \alpha_2 \cdots \alpha_r$*.*
  Par une récurrence immédiate, on obtient $\exists j \in [\![1, r]\!] : \pi \mid \alpha_j$*.*

► *L'implication réciproque découle directement de la transitivité de la divisibilité.*

12. **Décomposition en facteurs irréductibles.** Soit $\alpha \in \mathbb{Z}[i]$ non nul et non inversible.

(a) Montrer qu'il existe $r \in \mathbb{N}^*$ et $\pi_1, \dots, \pi_r \in \mathbb{Z}[i]$ irréductibles tels que $\alpha = \prod_{j=1}^{r} \pi_j$.

Pour tout $n \in \mathbb{N}^*$*, on note* $P(n)$ *l'assertion*

« quel que soit $\alpha \in \mathbb{Z}[i]$ *tel que* $1 < N(\alpha) \leqslant n$*, il existe* $r \in \mathbb{N}^*$ *et* $\pi_1, \dots, \pi_r \in \mathbb{Z}[i]$ *tel que*

$$\alpha = \prod_{j=1}^{r} \pi_j. \text{ »}$$

Montrons $\forall n \in \mathbb{N}^*, P(n)$ *par récurrence.*

Initialisation. *L'assertion* $P(1)$ *est tautologiquement vraie (car il n'existe pas de* $\alpha \in \mathbb{Z}[i]$ *tel que* $1 < N(\alpha) \leqslant 1$*).*

Hérédité. *Soit* $n \in \mathbb{N}^*$ *tel que* $P(n)$*.*

Soit $\alpha \in \mathbb{Z}[i]$ *tel que* $0 < N(\alpha) < n + 1$*. On distingue deux cas.*

► *Si* α *est irréductible,* $r = 1$ *et* $\pi_1 = \alpha$ *conviennent.*

► *Sinon, comme* α *n'est ni nul, ni inversible (car* $N(\alpha) > 1$*), on peut trouver* $\beta, \gamma \in \mathbb{Z}[i]$ *non inversibles tels que* $\alpha = \beta\gamma$*.*

En particulier, $N(\gamma) > 1$*, donc* $N(\beta) = \dfrac{N(\alpha)}{N(\gamma)} < N(\alpha) \leqslant n + 1$*. On obtient les mêmes inégalités en échangeant les rôles de* β *et* γ*, si bien que* $1 < N(\beta), N(\gamma) \leqslant n$*.*

D'après $P(n)$ *(et au prix d'une petite renumérotation), on peut trouver* $r, s \in \mathbb{N}^*$ *et* $\pi_1, \dots, \pi_r, \pi_{r+1}, \dots, \pi_s$ *irréductibles tels que*

$$\beta = \prod_{j=1}^{r} \pi_j \qquad \text{et} \qquad \gamma = \prod_{j=r+1}^{s} \pi_j,$$

donc $\alpha = \beta\gamma = \prod_{j=1}^{r+s} \pi_j$*,*

ce qui montre $P(n+1)$ *et clôt la récurrence.*

Étant donné un $\alpha \in \mathbb{Z}[i]$ *non nul et non inversible, on a* $1 < N(\alpha)$*, donc l'assertion* $P(N(\alpha))$ *conclut.*

(b) Soit $r, s \in \mathbb{N}^*$ et $\pi_1, \dots, \pi_r, \lambda_1, \dots, \lambda_s \in \mathbb{Z}[i]$ irréductibles tels que

$$\alpha = \prod_{j=1}^{r} \pi_j = \prod_{k=1}^{s} \lambda_k.$$

i. Montrer qu'il existe $k \in [\![1, s]\!]$ tel que π_r soit associé à λ_k.

On a $\pi_r \mid \prod_{k=1}^{s} \lambda_k$*. La question 11b montre alors l'existence de* $k \in [\![1, s]\!]$ *tel que* $\pi_r \mid \lambda_k$*.*

On peut donc trouver $\kappa \in \mathbb{Z}[i]$ *tel que* $\lambda_k = \kappa\pi_r$*.*

Par irréductibilité de λ_k *(et comme* π_r*, étant irréductible, ne saurait être inversible), on a nécessairement* $\kappa \in \mathbb{Z}[i]^\times$ *et donc* π_r *et* λ_k *associés.*

ii. Montrer $r = s$ et que l'on peut permuter les λ_k afin que, pour tout $j \in [\![1, r]\!]$, les irréductibles π_j et λ_j soient associés.

Pour tout $n \in \mathbb{N}^*$, on note $P(n)$ l'assertion

« quel que soit $m \in \mathbb{N}^*$, quels que soient $\xi_1, \dots, \xi_n, \zeta_1, \dots, \zeta_m \in \mathbb{Z}[i]$ irréductibles tels que l'on ait l'égalité $\prod_{j=1}^{n} \xi_j = \prod_{k=1}^{m} \zeta_k$, alors $n = m$ et, à permutation près, pour tout $j \in [\![1, n]\!]$, les irréductibles ξ_j et ζ_j sont associés. »

Montrons $\forall n \in \mathbb{N}^*, P(n)$ par récurrence.

Initialisation. *Soit $m \in \mathbb{N}^*$ et $\xi, \zeta_1, \dots, \zeta_m$ irréductibles tels que $\xi = \zeta_1 \cdots \zeta_m$.*

Si $m \geqslant 2$, on a $\xi = \zeta_1(\zeta_2 \cdots \zeta_m)$, où $N(\zeta_1) > 1$ et $N(\zeta_2 \cdots \zeta_m) = N(\zeta_2) \cdots N(\zeta_m) > 1$, ce qui contredit l'irréductibilité de ξ.

Ainsi, $m = 1$, et on a $\xi = \zeta_1$. A fortiori, ξ et ζ_1 sont associés.

Cela montre $P(1)$.

Hérédité. *Soit $n \in \mathbb{N}^*$ tel que $P(n)$. Montrons $P(n+1)$.*

Soit $m \in \mathbb{N}^*$ et $\xi_1, \dots, \xi_n, \xi_{n+1}, \zeta_1, \dots, \zeta_m \in \mathbb{Z}[i]$ irréductibles tels que $\prod_{j=1}^{n+1} \xi_j = \prod_{k=1}^{m} \zeta_k$.

D'après la question précédente, ξ_{n+1} est associé à un des facteurs du produit de droite. Quitte à les permuter, supposons ξ_{n+1} et ζ_m associés : on peut donc trouver $\varepsilon \in \mathbb{Z}[i]^\times$ tel que $\zeta_m = \varepsilon\, \xi_{n+1}$.

Comme $\prod_{j=1}^{n+1} N(\xi_j) = \prod_{k=1}^{m} N(\zeta_k)$ et que $N(\zeta_m) = N(\xi_{n+1}) > 1$, on peut simplifier et on obtient $1 < \prod_{j=1}^{n} N(\xi_j) = \prod_{k=1}^{m-1} N(\zeta_k)$. En particulier, le produit de droite n'est pas vide, et donc $m - 1 \in \mathbb{N}^*$.

La relation entre les deux produits se réécrit donc

$$\left(\prod_{j=1}^{n} \xi_j\right) \times \xi_{n+1} = \varepsilon \left(\prod_{k=1}^{m-1} \zeta_k\right) \times \xi_{n+1} \qquad \text{donc} \qquad \prod_{j=1}^{n} \xi_j = \prod_{k=1}^{m-1} \zeta'_k,$$

où l'on a posé $(\zeta'_1, \zeta'_2, \dots, \zeta'_{m-1}) = (\varepsilon\, \zeta_1, \zeta_2, \dots, \zeta_{m-1})$.

Remarquons que $\zeta'_1 = \varepsilon\, \zeta_1$ est encore irréductible : une décomposition de ζ'_1 comme un produit $\alpha'\, \beta'$ est simplement une décomposition $(\varepsilon\, \alpha)\, \beta$, où $\alpha\, \beta = \zeta_1$. La présence d'un inversible dans l'une des deux décompositions entraîne alors immédiatement la présence d'un inversible dans l'autre.

On peut alors appliquer $P(n)$: on obtient $n = m - 1$ et, à permutation près, $\xi_1, \dots, \xi_n$ sont associés à $\zeta'_1, \dots, \zeta'_n$ et donc aussi à $\zeta_1, \dots, \zeta_n$.

Ainsi, $n + 1 = m$ et, à permutation près, $\xi_1, \dots, \xi_{n+1}$ sont bien associés à $\zeta_1, \dots, \zeta_{n+1}$, ce qui montre $P(n+1)$, et clôt la récurrence.

Cela montre notamment le résultat demandé.

Partie II. Deux lemmes sur $\mathbb{F}_p$.

- Dans toute cette partie, p désigne un nombre premier impair, et $\mathbb{F}_p$ est le corps $\mathbb{Z}/p\mathbb{Z}$. On notera simplement 1 l'élément $1_{\mathbb{F}_p} = [1]_p$.
- On note $\mathbb{F}_p^\square = \left\{ x^2 \,\middle|\, x \in \mathbb{F}_p^\times \right\}$ l'ensemble des carrés non nuls dans $\mathbb{F}_p$.

13. (a) Montrer que $q : \begin{cases} \mathbb{F}_p^\times & \to \mathbb{F}_p^\times \\ x & \mapsto x^2 \end{cases}$ est un morphisme de groupes, dont on déterminera le noyau.

- *Soit $x, y \in \mathbb{F}_p^\times$. On a*

$$q(xy) = (xy)^2 = x^2 y^2 = q(x)\, q(y),$$

donc q est un morphisme de groupes (multiplicatifs).
- *Soit $x \in \ker q$. On a donc $x^2 = 1$, c'est-à-dire $(x-1)(x+1) = 0$.*
Comme $\mathbb{F}_p$ est notamment intègre, on en déduit $x - 1 = 0$ ou $x + 1 = 0$, donc $x \in \{\pm 1\}$.
Réciproquement, $q(1) = q(-1) = 1$, donc $\ker q = \{\pm 1\}$.

(b) En déduire que $\mathbb{F}_p^\square$ possède exactement $\dfrac{p-1}{2}$ éléments.

Comme $p > 2$, les éléments -1 et 1 de $\mathbb{F}_p^\times$ sont bien différents, donc $|\ker q| = 2$.
La relation $\left|\mathbb{F}_p^\times\right| = |\ker q| \times |\operatorname{im} q|$ et le fait que $\mathbb{F}_p^\square = \operatorname{im} q$, par définition de q, montrent alors

$$\left|\mathbb{F}_p^\square\right| = \frac{1}{2}\left|\mathbb{F}_p^\times\right| = \frac{p-1}{2}.$$

14. En considérant $Q = \left\{ a^2 \,\middle|\, a \in \mathbb{F}_p \right\}$ et $\left\{ -1 - b^2 \,\middle|\, b \in \mathbb{F}_p \right\}$, montrer le résultat suivant.

Lemme A. Il existe $a, b \in \mathbb{F}_p$ tels que $a^2 + b^2 = -1$.

Remarquons que $Q = \left\{ a^2 \,\middle|\, a \in \mathbb{F}_p \right\} = \{0\} \cup \mathbb{F}_p^\times$ possède $1 + \dfrac{p-1}{2} = \dfrac{p+1}{2}$ éléments.
L'application $f : t \mapsto -1 - t$ est involutive, donc c'est une bijection $\mathbb{F}_p \to \mathbb{F}_p$. En particulier, elle induit une bijection $Q \to f[Q] = \left\{ -1 - b^2 \,\middle|\, b \in \mathbb{F}_p \right\}$.
En particulier, $\left|\left\{ -1 - b^2 \,\middle|\, b \in \mathbb{F}_p \right\}\right| = \dfrac{p+1}{2}$.
En particulier, $|Q| + \left|\left\{ -1 - b^2 \,\middle|\, b \in \mathbb{F}_p \right\}\right| = p + 1 > |\mathbb{F}_p|$, ce qui montre que Q et $\left\{ -1 - b^2 \,\middle|\, b \in \mathbb{F}_p \right\}$ ne peuvent pas être disjoints.
On peut donc trouver $a, b \in \mathbb{F}_p$ tels que $a^2 = -1 - b^2$, ce qui donne $a^2 + b^2 = -1$, et conclut.

15. Le but de cette question est de montrer le résultat suivant (qui a d'ailleurs été admis lors de la deuxième composition).

Lemme B. $-1 \in \mathbb{F}_p^\square$ si et seulement si $p \equiv 1 \pmod 4$.

(a) Montrer l'implication $-1 \in \mathbb{F}_p^\square \Rightarrow p \equiv 1 \pmod 4$, en étudiant l'ordre de -1 dans le groupe multiplicatif $\mathbb{F}_p^\times$.

- *On a clairement $(-1)^2 = 1$ mais $-1 \neq 1$ (notons que cette non-égalité a lieu dans $\mathbb{F}_p$, c'est-à-dire qu'il s'agit plus élémentairement de la non-congruence $-1 \not\equiv 1 \pmod p$: on utilise ici l'imparité de p), ce qui montre que l'ordre de -1 est 2.*

- ▶ *Supposons* $-1 \in \mathbb{F}_p^\square$. *D'après le théorème de Lagrange, l'ordre de* -1 *(c'est-à-dire* 2*) doit diviser* $\left|\mathbb{F}_p^\square\right| = \dfrac{p-1}{2}$, *ce qui donne* $4 \mid p-1$, *et donc* $p \equiv 1 \pmod 4$.

(b) On suppose maintenant $p \equiv 1 \pmod 4$.

i. Montrer que $i : \begin{cases} \mathbb{F}_p^\square \to \mathbb{F}_p^\square \\ x \mapsto x^{-1} \end{cases}$ est une involution bien définie.

On a déjà vu que $\mathbb{F}_p^\square = \operatorname{im} q$ *est un sous-groupe de* $\mathbb{F}_p^\times$. *À ce titre, il est stable par passage à l'inverse et l'application* i *est bien définie.*
Son caractère involutif est évident.

ii. Montrer que l'ensemble $\left\{x \in \mathbb{F}_p^\square \,\middle|\, i(x) = x\right\}$ des points fixes de i est de cardinal pair.

- ▶ *Considérons une involution* j *sur un ensemble fini quelconque* X.
Pour tout $x \in X$, *on a* $j\big(j(x)\big) = x$ *: autrement dit, si* $y = j(x)$, *on a* $x = j(y)$.
Pour tout $x \in X$, *on a donc deux possibilités :*
  - *soit* x *est un* point fixe, *c'est-à-dire que* $j(x) = x$;
  - *soit il existe* $y \neq x$ *tel que* $j(x) = y$ *et* $j(y) = x$.

  Ainsi, on peut décomposer l'ensemble X *en* $r \in \mathbb{N}$ *points fixes* $x_1, \dots, x_r$ *et* s *paires* $\{y_1, z_1\}, \dots, \{y_s, z_s\}$ *dont les deux éléments sont échangés par* j.
  En particulier, on a $|X| = r + 2s$ *: le nombre de points fixes de l'involution est de même parité que le cardinal* $|X|$.
- ▶ *Ici,* $\left|\mathbb{F}_p^\square\right| = \dfrac{p-1}{2}$ *est pair (parce que* $p \equiv 1 \pmod 4$*), donc l'involution* i *possède un nombre pair de points fixes.*

iii. Conclure la démonstration du lemme B.

On a déjà montré le sens direct. Supposons donc $p \equiv 1 \pmod 4$ *et montrons que* $-1 \in \mathbb{F}_p^\square$.

- ▶ *D'après la question précédente, l'involution* i *possède un nombre pair de points fixes. Il est clair que* $1 = 1^2 \in \mathbb{F}_p^\square$ *en est un.*
On peut donc trouver $x \in \mathbb{F}_p^\square$, *différent de* 1, *tel que* $i(x) = x$
- ▶ *On a ainsi* $x = i(x) = x^{-1}$, *ce qui donne* $x^2 = 1$, *ou encore* $(x-1)(x+1) = 0$.
Comme $x \neq 1$, *on en déduit* $x = -1$, *ce qui montre* $-1 \in \mathbb{F}_p^\square$, *et conclut la démonstration du lemme B.*

Partie III. Irréductibles dans $\mathbb{Z}[i]$.

16. Soit $\pi \in \mathbb{Z}[i]$ irréductible.
Constater que $\pi \mid \pi\overline{\pi}$ et en déduire l'existence d'un nombre premier p tel que $\pi \mid p$.

Le produit $n = \pi\overline{\pi} = N(\pi)$ *est une norme, donc un entier naturel.*
Comme π *est irréductible, on a même* $n = N(\pi) > 1$.
On écrit alors la décomposition en facteurs premiers (en répétant les facteurs premiers plutôt qu'en utilisant les exposants) : on peut trouver r *nombres premiers* $p_1, \dots, p_r$ *tels que* $\pi \mid n = p_1 \cdots p_r$.
D'après la question 11b, on peut donc trouver $j \in [\![1, r]\!]$ *tel que* $\pi \mid p_j$, *ce qui conclut.*

Cette question montre que, pour déterminer les éléments irréductibles de $\mathbb{Z}[i]$, il suffit de savoir factoriser dans $\mathbb{Z}[i]$ tous les nombres premiers p. C'est le but de cette partie.
Le cas $p = 2$ ayant déjà été traité, on se concentrera sur celui des nombres premiers impairs.

17. Soit p un nombre premier tel que $p \equiv 3 \pmod 4$.

(a) Montrer que p n'est pas la somme de deux carrés parfaits.

Supposons par l'absurde que p *soit la somme de deux carrés parfaits.*
On peut donc trouver $n, m \in \mathbb{N}$ *tels que* $p = n^2 + m^2$. *Or,* [2]

- *si* $n \equiv 0 \pmod 4$, $n^2 \equiv 0 \pmod 4$;
- *si* $n \equiv 1 \pmod 4$, $n^2 \equiv 1 \pmod 4$;
- *si* $n \equiv 2 \pmod 4$, $n^2 \equiv 0 \pmod 4$;
- *si* $n \equiv 3 \pmod 4$, $n^2 \equiv 1 \pmod 4$.

La même chose valant pour m, *on obtient* $n^2 + m^2 \not\equiv 3 \pmod 4$ *et fournit une contradiction.*

(b) En déduire que p est un élément irréductible de $\mathbb{Z}[i]$.

La même démonstration que dans le cas $p = 3$ *convient : en passant à la norme, l'égalité* $p = \alpha\beta$ *donne* $N(\alpha)N(\beta) = p^2$, *et il est impossible que* $N(\alpha) = (\text{Ré}\,\alpha)^2 + (\text{Im}\,\alpha)^2 = p$ *d'après la question précédente, donc* $N(\alpha) = 1$ *ou* $N(\beta) = 1$, *ce qui conclut.*

18. Soit p un nombre premier tel que $p \equiv 1 \pmod 4$.

(a) Montrer qu'il existe un entier $n \in \mathbb{Z}$ tel que $p \mid n^2 + 1$, mais que $p \nmid n \pm i$.

D'après le lemme B, $-1 \in \mathbb{F}_p^\square$. *On peut donc trouver* $x \in \mathbb{F}_p^\times$ *tel que* $x^2 = -1$.
On peut également trouver $n \in \mathbb{Z}$ *tel que* $x = [n]_p$, *si bien que l'égalité précédente donne* $n^2 \equiv -1 \pmod p$. *Autrement dit,* $p \mid n^2 + 1$.
Enfin, le nombre premier p *ne peut pas diviser* $n \pm i$ *(dans* $\mathbb{Z}[i]$*) : d'après la question 5a, cela entraînerait que* p *divise* ± 1 *(dans* $\mathbb{Z}$*), ce qui est absurde.*

(b) En déduire que p n'est pas un élément irréductible de $\mathbb{Z}[i]$.

Si p *était irréductible, les assertions* $p \mid n^2 + 1 = (n - i)(n + i)$ *et* $p \nmid n \pm i$ *contrediraient directement la question 11b.*

(c) Montrer qu'il existe $\pi_1, \pi_2 \in \mathbb{Z}[i]$ irréductibles tels que $p = \pi_1\,\pi_2$.

Comme $N(p) = p^2 > 1$, *l'élément* p *de* $\mathbb{Z}[i]$ *n'est ni nul ni inversible.*
On utilise le résultat de la partie I : il existe $r \in \mathbb{N}^*$ *et* $\pi_1, \ldots, \pi_r \in \mathbb{Z}[i]$ *irréductibles tels que* $p = \pi_1 \cdots \pi_r$. *Comme* p *n'est pas irréductible, on a nécessairement* $r \geqslant 2$.
En passant à la norme, on obtient $p^2 = N(p) = N(\pi_1) \cdots N(\pi_r)$.
Par irréductibilité, on a $\forall j \in [\![1, r]\!], N(\pi_j) > 1$, *donc les normes apparaissant dans le produit précédent sont des diviseurs stricts de* p^2.
Puisque p *est premier, il y a une seule possibilité : on a* $r = 2$ *et* $N(\pi_1) = N(\pi_2) = p$.

2. On peut économiser un cas en remarquant que $3 \equiv -1 \pmod 4$. Il est même possible de montrer directement les implications $n \equiv 0 \pmod 2 \Rightarrow n^2 \equiv 0 \pmod 4$ et $n \equiv 1 \pmod 2 \Rightarrow n^2 \equiv 1 \pmod 4$ en revenant aux définitions.

Partie IV. Théorème des deux carrés (Fermat, ~1640 ? ; Euler, 1749).

On considère l'ensemble

$$\mathcal{S}_2 = \left\{ a^2 + b^2 \,\middle|\, a, b \in \mathbb{Z} \right\}.$$

On va montrer le *théorème des deux carrés de Fermat-Euler* : un entier $n \in \mathbb{N}^*$ appartient à $\mathcal{S}_2$ si et seulement s'il vérifie la condition suivante :

pour tout nombre premier $\ell \equiv 3 \pmod 4$, la valuation ℓ-adique $v_\ell(n)$ est paire. $(*)$

19. Montrer que l'ensemble $\mathcal{S}_2$ est stable par produit.

Remarquons que $\mathcal{S}_2$ peut également s'écrire $\mathcal{S}_2 = \{N(\alpha) \mid \alpha \in \mathbb{Z}[i]\}$.
Pour plus de commodité, nous utiliserons cette écriture.
Soit $n, m \in \mathcal{S}_2$. On peut donc trouver $\alpha, \beta \in \mathbb{Z}[i]$ tels que $n = N(\alpha)$ et $m = N(\beta)$.
On a alors

$$nm = N(\alpha)\,N(\beta) = N(\underbrace{\alpha\,\beta}_{\in \mathbb{Z}[i]}) \in \mathcal{S}_2,$$

ce qui conclut.

20. (a) En utilisant la partie III, montrer que tout nombre premier $p \equiv 1 \pmod 4$ appartient à $\mathcal{S}_2$.

La dernière question de la partie III a montré que tout premier $p \equiv 1 \pmod 4$ possédait une décomposition en facteurs irréductibles $p = \pi_1\,\pi_2$ dans $\mathbb{Z}[i]$ telle que $N(\pi_1) = N(\pi_2) = p$.
En particulier, p est la norme d'un élément de $\mathbb{Z}[i]$, donc il s'agit d'un élément de $\mathcal{S}_2$.

(b) En déduire que si un entier $n \in \mathbb{N}^*$ vérifie la condition $(*)$, alors $n \in \mathcal{S}_2$.

Soit $n \in \mathbb{N}^*$ vérifiant la condition $(*)$. On va écrire sa décomposition en facteurs premiers en notant $p_1, \dots, p_r$ (resp. $\ell_1, \dots, \ell_s$) les nombres premiers impairs congrus à 1 (resp. 3) modulo 4 intervenant dans sa décomposition en facteurs premiers :

$$n = 2^{v_2(n)} \prod_{j=1}^{r} p_j^{v_{p_j}(n)} \prod_{k=1}^{s} \ell_k^{v_{\ell_k}(n)}.$$

- *On a $2 = 1^2 + 1^2$ (ou $2 = N(1+i)$), donc $2 \in \mathcal{S}_2$.*
  Par application répétée de la stabilité par produit (ou trivialement si $v_2(n) = 0$), on en déduit que $2^{v_2(n)} \in \mathcal{S}_2$.
- *Pour tout $j \in [\![1, r]\!]$, la question précédente entraîne que $p_j \in \mathcal{S}_2$, et donc que $p_j^{v_{p_j}(n)} \in \mathcal{S}_2$.*
- *Soit $k \in [\![1, s]\!]$. Par hypothèse, la valuation $v_{\ell_k}(n)$ est paire, et on va l'écrire $2w_k$.*
  On a évidemment $\ell_k^2 = \ell_k^2 + 0^2 = N(\ell_k) \in \mathcal{S}_2$.
  Par stabilité par produit, $\left(\ell_k^2\right)^{w_k} = \ell_k^{2w_k} = \ell_k^{v_{\ell_k}(n)} \in \mathcal{S}_2$.

Par stabilité par produit, $n \in \mathcal{S}_2$.

21. Soit p un nombre premier tel que $p \equiv 3 \pmod 4$ et $a, b \in \mathbb{Z}$.
Montrer $p \mid a^2 + b^2 \Rightarrow \big(p \mid a + ib \text{ et } p \mid a - ib\big)$.

Supposons $p \mid a^2 + b^2$.
Comme $a^2 + b^2 = (a + ib)(a - ib)$ et que p est irréductible (question 17b), la question 11b entraîne que $p \mid a + ib$ ou $p \mid a - ib$.

- *Dans le premier cas, on peut trouver* $\kappa \in \mathbb{Z}[i]$ *tel que* $a + ib = \kappa p$. *En passant au conjugué, on obtient* $a - ib = \overline{\kappa} p$, *ce qui montre que* $p \mid a - ib$, *car* $\overline{\kappa} \in \mathbb{Z}[i]$.
- *La même démonstration montre que, dans le deuxième cas, on a également* $p \mid a + ib$.

Ainsi, $p \mid a + ib$ *et* $p \mid a - ib$.

22. Conclure la démonstration du théorème des deux carrés.

Il reste à montrer que pour tout $n \in \mathcal{S}_2$ *non nul et tout premier* $p \equiv 3 \pmod 4$, *la valuation* $v_p(n)$ *est impaire.*

On suppose par l'absurde que c'est faux : on peut donc trouver un nombre premier $p \equiv 3 \pmod 4$ *tel que l'ensemble*

$$\{k \in \mathbb{N} \mid \exists n \in \mathbb{N} : v_p(n) = 2k + 1\}$$

soit non vide. On peut donc considérer son minimum k, *et un entier* $n \in \mathcal{S}_2$ *tel que* $v_p(n) = 2k + 1$.

Autrement dit, n *possède une valuation* p*-adique impaire, et minimale parmi les valuations* p*-adiques impaires des éléments de* $\mathcal{S}_2$.

En particulier, $v_p(n) > 0$, *ce qui montre que* $p \mid n$. *Comme* $n \in \mathcal{S}_2$, *on peut trouver* $a, b \in \mathbb{Z}$ *tels que* $n = a^2 + b^2$.

D'après la question précédente, on a $p \mid a + ib$.

D'après 5a, le nombre premier p *divise* a *et* b *dans* $\mathbb{Z}$.

On en déduit que $\dfrac{a}{p}, \dfrac{b}{p} \in \mathbb{Z}$, *et donc que*

$$n = a^2 + b^2 = p^2 \left(\left(\frac{a}{p} \right)^2 + \left(\frac{b}{p} \right)^2 \right).$$

L'entier $n' = \left(\dfrac{a}{p} \right)^2 + \left(\dfrac{b}{p} \right)^2$ *est donc un élément de* $\mathcal{S}_2$, *et on a*

$$v_p(n) = v_p(p^2) + v_p(n') = 2 + n',$$

ce qui montre que $v_p(n')$ *est impaire et* $< v_p(n)$, *ce qui contredit la définition de* n, *et conclut la démonstration.*

Partie V. Hamilton, Hurwitz et Lagrange.

► On considère l'ensemble des *quaternions* (*de Hamilton*)

$$\mathbb{H} = \left\{ \begin{pmatrix} z_1 & -z_2 \\ \overline{z}_2 & \overline{z}_1 \end{pmatrix} \,\middle|\, z_1, z_2 \in \mathbb{C} \right\}$$

et on note $\quad 1_{\mathbb{H}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad K = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix},$

de telle sorte que, pour tous $t, x, y, z \in \mathbb{R}$, $\begin{pmatrix} t+ix & -y-iz \\ y-iz & t-ix \end{pmatrix} = t\,1_{\mathbb{H}} + x\,I + y\,J + z\,K$.

► On appelle *demi-entier* tout nombre de la forme $\dfrac{1}{2} + k$, où $k \in \mathbb{Z}$.
On note $\mathcal{O}$ (et on appelle *ordre des quaternions de Hurwitz*) l'ensemble des quaternions de la forme $t\,1_{\mathbb{H}} + x\,I + y\,J + z\,K$ où les nombres réels t, x, y et z sont tous entiers, ou bien tous demi-entiers.

23. Montrer que $\mathbb{H}$ est un sous-anneau non commutatif de $M_2(\mathbb{C})$.

► *L'unité multiplicative de* $M_2(\mathbb{C})$ *est* $1_{\mathbb{H}} \in \mathbb{H}$.

► *Soit* $q, r \in \mathbb{H}$. *On peut trouver* $z_1, z_2, w_1, w_2 \in \mathbb{C}$ *tels que*

$$q = \begin{pmatrix} z_1 & -z_2 \\ \overline{z}_2 & \overline{z}_1 \end{pmatrix} \qquad \textit{et} \qquad r = \begin{pmatrix} w_1 & -w_2 \\ \overline{w}_2 & \overline{w}_1 \end{pmatrix}.$$

- *On a alors* $q - r = \begin{pmatrix} z_1 - w_1 & -(z_2 - w_2) \\ \overline{z_2 - w_2} & \overline{z_1 - w_1} \end{pmatrix} \in \mathbb{H}$;
- *On a* $qr = \begin{pmatrix} z_1w_1 - z_2\overline{w_2} & -z_1w_2 - z_2\overline{w_1} \\ \overline{z_2}w_1 + \overline{z_1}w_2 & -\overline{z_2}w_2 + \overline{z_1}w_1 \end{pmatrix} = \begin{pmatrix} z_1w_1 - z_2\overline{w_2} & -(z_1w_2 + z_2\overline{w_1}) \\ \overline{z_1w_2 + z_2\overline{w_1}} & \overline{z_1w_1 - z_2\overline{w_2}} \end{pmatrix} \in \mathbb{H}$.

Cela montre déjà que $\mathbb{H}$ *est un sous-anneau de* $M_2(\mathbb{C})$.

► *On a* $IJ = K \neq -K = JI$, *donc cet anneau n'est pas commutatif.*

24. Pour tout $M \in M_2(\mathbb{C})$, on note $M^* = \overline{M}^T$.

(a) Montrer que, pour tout $q \in \mathbb{H}$, on a $q^* \in \mathbb{H}$ et les égalités $q\,q^* = q^*\,q = \det(q)\,1_{\mathbb{H}}$.

C'est un calcul direct.

(b) L'application $q \mapsto q^*$ est-elle un endomorphisme d'anneaux de $\mathbb{H}$?

Non, à cause de la non-commutativité de $\mathbb{H}$.
Par exemple, on a $(IJ)^* = K^* = -K$ *alors que* $I^*J^* = (-I)(-J) = IJ = K$.
En revanche, il est vrai que $\forall q, r \in \mathbb{H}, (qr)^* = r^*q^*$.

(c) Montrer que $\mathbb{H}^\times = \mathbb{H} \setminus \{0\}$.

► *Pour tout* $q \in \mathbb{H}$, *on a* $0\,q = 0 \neq 1_{\mathbb{H}}$, *donc* 0 *n'est pas inversible.*
Cela montre l'inclusion directe.

► *Soit* $q \in \mathbb{H} \setminus \{0\}$.

On peut donc trouver $z_1, z_2 \in \mathbb{C}$ *non tous les deux nuls tels que* $q = \begin{pmatrix} z_1 & -z_2 \\ \overline{z_2} & \overline{z_1} \end{pmatrix}$.

On a alors $\det(q) = |z_1|^2 + |z_2|^2 > 0$, *ce qui montre que* $q \in GL_2(\mathbb{C})$.
Par ailleurs, les formules de la question 24a montrent que son inverse est alors

$$q^{-1} = \frac{1}{\det q} q^* \in \mathbb{H},$$

ce qui montre que $q \in \mathbb{H}^\times$ *et conclut.*

(d) Peut-on en déduire que $\mathbb{H}$ est un corps ?

Non, car $\mathbb{H}$ n'est pas commutatif ! L'anneau des quaternions est le prototype de « corps gauche », de « corps non commutatif » ou « d'algèbre à division », c'est-à-dire d'anneau non nul dans lequel tout élément non nul possède un inverse. La structure de ces objets est passionnante, mais l'usage actuel est plutôt de ne pas les qualifier de corps.

25. Montrer que $\mathcal{O}$ est un sous-anneau non commutatif de $\mathbb{H}$, et montrer que $\forall q \in \mathcal{O}, \text{dét}(q) \in \mathbb{N}$.

Simplifions un peu les calculs en introduisant le sous-ensemble

$$\mathcal{O}' = \{t\,1_{\mathbb{H}} + x\,I + y\,J + z\,K \mid t, x, y, z \in \mathbb{Z}\} = \left\{ \begin{pmatrix} z_1 & -\overline{z_2} \\ z_2 & \overline{z_1} \end{pmatrix} \,\middle|\, z_1, z_2 \in \mathbb{Z}[i] \right\} \subseteq \mathcal{O},$$

dont les calculs de la question 23 montrent directement qu'il s'agit d'un sous-anneau de $\mathbb{H}$.
Fixons maintenant $\omega = \dfrac{1+I+J+K}{2} = \dfrac{1}{2}\begin{pmatrix} 1+i & -1-i \\ 1-i & 1-i \end{pmatrix} \in \mathcal{O} \setminus \mathcal{O}'$, de telle sorte que

$$\mathcal{O} = \mathcal{O}' \cup \left\{ q + \omega \,\middle|\, q \in \mathcal{O}' \right\}.$$

- *Il est clair que $0 \in \mathcal{O}$ et que $\mathcal{O}$ est stable par passage à l'opposé.*
- *La stabilité par somme est claire, à l'aide d'une disjonction de cas : étant donné $q, q' \in \mathcal{O}'$, on a*
  - $q + q' \in \mathcal{O}' \subseteq \mathcal{O}$;
  - $(\omega + q) + q' = q + (\omega + q') = \omega + \underbrace{(q + q')}_{\in \mathcal{O}'} \in \mathcal{O}$;
  - $(\omega + q) + (\omega + q') = \underbrace{1 + I + J + K}_{\in \mathcal{O}'} + q + q' \in \mathcal{O}' \subseteq \mathcal{O}$.

Cela montre déjà que $\mathcal{O}$ est un sous-groupe additif de $\mathbb{H}$.

- *Clairement, $1_{\mathbb{H}} \in \mathcal{O}' \subseteq \mathcal{O}$.*
- *Reste à montrer la stabilité par produit.*
  - *On a clairement $\forall q, q' \in \mathcal{O}', q\,q' \in \mathcal{O}' \subseteq \mathcal{O}$.*
  - *On vérifie facilement mais laborieusement que $I\,\omega, J\,\omega, K\,\omega, \omega\,I, \omega\,J, \omega\,K \in \mathcal{O}$. Pour ce genre de calculs, la « table de multiplication » suivante est d'une aide précieuse.*

$\cdot$	$1_{\mathbb{H}}$	I	J	K
$1_{\mathbb{H}}$	$1_{\mathbb{H}}$	I	J	K
I	I	$-1_{\mathbb{H}}$	K	$-J$
J	J	$-K$	$-1_{\mathbb{H}}$	I
K	K	J	$-I$	$-1_{\mathbb{H}}$

  Par stabilité par somme, on en déduit $\forall q \in \mathcal{O}', \big(q\,\omega \in \mathcal{O}$ et $\omega\,q \in \mathcal{O}\big)$.
  - *On a $\omega^2 = \omega - 1_{\mathbb{H}} \in \mathcal{O}$ (ce calcul un peu pénible est évitable à l'aide du théorème de Cayley-Hamilton, car $\text{tr}(\omega) = \text{dét}(\omega) = 1$).*

À l'aide de ces « briques de base », on vérifie facilement, par une petite disjonction de cas, que $\mathcal{O}$ est stable par produit.

Cela conclut la démonstration du fait que $\mathcal{O}$ est un sous-anneau de $\mathbb{H}$, et le « contre-exemple » $IJ \neq JI$ continue à montrer sa non-commutativité.
Enfin, soit t, x, y, z tous entiers ou tous demi-entiers. On note $q = t\,1_{\mathbb{H}} + x\,I + y\,J + z\,K$. On a

$$\text{dét}(q) = t^2 + x^2 + y^2 + z^2.$$

Ainsi,

- *si* t, x, y, z *sont tous entiers, on a clairement* $\text{dét}(q) \in \mathbb{N}$;
- *si* t, x, y, z *sont tous demi-entiers, on a*

$$\text{dét}(q) = \frac{(2t)^2 + (2x)^2 + (2y)^2 + (2z)^2}{4}.$$

Les éléments $2t, 2x, 2y, 2z$ *sont tous impairs, donc* $(2t)^2 \equiv (2x)^2 \equiv (2y)^2 \equiv (2z)^2 \equiv 1 \pmod 4$, *ce qui montre*

$$(2t)^2 + (2x)^2 + (2y)^2 + (2z)^2 \equiv 0 \pmod 4 \qquad \textit{et donc} \qquad \text{dét}(q) \in \mathbb{N}.$$

26. Montrer que $\mathcal{O}^\times = \{q \in \mathcal{O} \mid \text{dét}(q) = 1\}$ et déterminer exactement les éléments de $\mathcal{O}^\times$.

- *Montrons* $\mathcal{O}^\times = \{q \in \mathcal{O} \mid \text{dét}(q) = 1\}$.
  - *Soit* $q \in \mathcal{O}^\times$. *On a donc* q *inversible et* $q^{-1} \in \mathcal{O}$.
    La multiplicativité du déterminant et la question précédente montrent

$$1 = \text{dét}(1_{\mathbb{H}}) = \underbrace{\text{dét}(q)}_{\in\mathbb{N}} \underbrace{\text{dét}(q^{-1})}_{\in\mathbb{N}},$$

    donc $\text{dét}(q) = 1$.
  - *Soit* $q \in \mathcal{O}$ *tel que* $\text{dét}(q) = 1$.
    On a alors $q \in \mathbb{H}^\times$ *et* $q^{-1} = \dfrac{1}{\text{dét}(q)} q^* = q^* \in \mathcal{O}$, *donc* $q \in \mathcal{O}^\times$.
- *Soit* $q = t\,1_{\mathbb{H}} + x\,I + y\,J + z\,K \in \mathcal{O}$. *Déterminons à quelle condition* $1 = \text{dét}(q) = t^2 + x^2 + y^2 + z^2$.
  - *Dans le cas où les quatre coordonnées sont entières, on doit avoir l'une d'entre elles qui vaut* ± 1, *et les autres doivent être nulles.*
    Cela fournit déjà huit éléments de $\mathcal{O}^\times$.
  - *Dans le cas où les quatre coordonnées sont demi-entières, on doit avoir, comme dans la question précédente,*

$$(2t)^2 + (2x)^2 + (2y)^2 + (2z)^2 = 4 \qquad \textit{et} \qquad 2t \equiv 2x \equiv 2y \equiv 2z \equiv 1 \pmod 2,$$

    ce qui se produit si et seulement si $2t, 2x, 2y, 2z = \pm 1$.
    Cela fournit seize autres éléments de $\mathcal{O}^\times$.

  Ainsi,

$$\mathcal{O}^\times = \left\{ \pm 1_{\mathbb{H}}, \pm I, \pm J, \pm K, \frac{\pm 1_{\mathbb{H}} \pm I \pm J \pm K}{2} \right\}.$$

27. **Arithmétique dans** $\mathcal{O}$**.**

(a) Montrer que $\forall z \in \mathbb{H}, \exists \kappa \in \mathcal{O} : \text{dét}(\kappa - z) < 1$.

Soit $z \in \mathbb{H}$. *On peut trouver* $t, x, y, z \in \mathbb{R}$ *tels que* $z = t\,1_{\mathbb{H}} + x\,I + y\,J + z\,K$.
On peut trouver $u, a, b, c \in \mathbb{Z}$ *tels que* $|t - u|, |x - a|, |y - b|, |z - c| \leqslant \dfrac{1}{2}$.
On a alors

$$\text{dét}\left(z - \left(u\,1_{\mathbb{H}} + a\,I + b\,J + c\,K\right)\right) = (t-u)^2 + (x-a)^2 + (y-b)^2 + (z-c)^2 \leqslant 4 \times \frac{1}{4} \leqslant 1.$$

On distingue alors deux cas :

- *si l'inégalité ci-dessus est stricte,* $\kappa = u\,1_{\mathbb{H}} + a\,I + b\,J + c\,K \in \mathcal{O}' \subseteq \mathcal{O}$ *convient ;*

► *si l'inégalité ci-dessus est une égalité, on a entre autres*

$$|t-u| = |x-a| = |y-b| = |z-c| = \frac{1}{2},$$

ce qui montre que t, x, y *et* z *sont tous demi-entiers, donc* $z \in \mathcal{O}$ *et* $\kappa = z$ *convient clairement.*

(b) En déduire que pour tous $\alpha, \beta \in \mathcal{O}$ tels que $\beta \neq 0$, il existe $\kappa, \rho \in \mathcal{O}$ tels que

$$\alpha = \kappa\,\beta + \rho \qquad \text{et} \qquad \text{dét}(\rho) < \text{dét}(\beta).$$

On reprend essentiellement mot pour mot la question 9b.
Soit $\alpha, \beta \in \mathcal{O}$ *tels que* $\beta \neq 0$. *Posons* $z = \alpha\,\beta^{-1} \in \mathbb{H}$.
D'après la question précédente, on peut trouver $\kappa \in \mathcal{O}$ *tel que* $\text{dét}\,(z-\kappa) < 1$.
Ainsi,

$$\text{dét}(\alpha - \kappa\,\beta) = \text{dét}\left(\alpha\beta^{-1} - \kappa\right)\,\text{dét}\,(\beta) < \text{dét}(\beta),$$

ce qui conclut (en posant $\rho = \alpha - \kappa\,\beta$, *ce qui rend l'égalité* $\alpha = \kappa\,\beta + \rho$ *tautologique).*

Comme dans le cas de $\mathbb{Z}[i]$, la dernière question entraîne que pour tous $\alpha, \beta \in \mathcal{O}$ non tous les deux nuls, il existe $\delta \in \mathcal{O}$ tel que $\underbrace{\{\lambda\,\alpha + \mu\,\beta \,|\, \lambda, \mu \in \mathcal{O}\}}_{(\alpha,\beta)} = \underbrace{\{\nu\,\delta \,|\, \nu \in \mathcal{O}\}}_{(\delta)}$. On ne demande pas de le vérifier.

On pourra noter que la démonstration donnée à la question 10 n'utilise pas la commutativité de l'anneau $\mathbb{Z}[i]$ *: elle se traduit* verbatim *dans le contexte non commutatif de l'anneau* $\mathcal{O}$.

28. **Théorème des quatre carrés (Lagrange, 1770 ; démonstration de Hurwitz, 1896).** Notons

$$\mathcal{S}_4 = \left\{ a^2 + b^2 + c^2 + d^2 \;\middle|\; a, b, c, d \in \mathbb{Z} \right\}.$$

(a) Montrer que $\mathcal{S}_4$ est stable par produit.

Comme

$$\text{dét}\begin{pmatrix} t+ix & -(y+iz) \\ y-iz & t-ix \end{pmatrix} = t^2 + x^2 + y^2 + z^2,$$

on peut également donner une présentation alternative de $\mathcal{S}_4$ *:*

$$\mathcal{S}_4 = \left\{ \text{dét}(q) \;\middle|\; q \in \mathcal{O}' \right\}.$$

Cela conclut directement : soit $n, m \in \mathcal{S}_4$. *On peut donc trouver* $q, q' \in \mathcal{O}'$ *tels que* $n = \text{dét}(q)$ *et* $m = \text{dét}(q')$. *Comme* $q\,q' \in \mathcal{O}'$, *on a*

$$nm = \text{dét}(q)\,\text{dét}(q') = \text{dét}(qq') \in \mathcal{S}_4.$$

Remarque. *Si on a le courage, on peut transformer cette démonstration en une formule explicite, la* formule des quatre carrés d'Euler *: pour tous* $t_1, x_1, y_1, z_1, t_2, x_2, y_2, z_2 \in \mathbb{Z}$, *on a*

$$\begin{aligned}\left(t_1^2 + x_1^2 + y_1^2 + z_1^2\right)\left(t_2^2 + x_2^2 + y_2^2 + z_2^2\right) = {} & (t_1t_2 - x_1x_2 - y_1y_2 - z_1z_2)^2 \\ & + (t_1x_2 + x_1t_2 + y_1z_2 - z_1y_2)^2 \\ & + (t_1y_2 - x_1z_2 + y_1t_2 + z_1x_2)^2 \\ & + (t_1z_2 + x_1y_2 - y_1x_2 + z_1t_2)^2.\end{aligned}$$

(b) Montrer que $\mathcal{S}_4 = \{\text{dét}(q) \mid q \in \mathcal{O}\}$.

- *On a vu à la question précédente que* $\mathcal{S}_4 = \left\{\text{dét}(q) \,\middle|\, q \in \mathcal{O}'\right\}$, *ce qui montre* $\mathcal{S}_4 \subseteq \{\text{dét}(q) \mid q \in \mathcal{O}\}$.
- *Réciproquement, soit* $n \in \{\text{dét}(q) \mid q \in \mathcal{O}\}$. *On peut trouver* $q \in \mathcal{O}$ *tel que* $n = \text{dét}(q)$.
  - *Si* $q \in \mathcal{O}'$, *on a clairement* $n \in \mathcal{S}_4$.
  - *Si* $q \in \mathcal{O} \setminus \mathcal{O}'$, *ses quatre coordonnées sont des demi-entiers.*

    Or, tout demi entier peut s'écrire de la forme $2k \pm \dfrac{1}{2}$, *pour un entier* $k \in \mathbb{Z}$ *et un signe bien choisi. En effectuant cette décomposition coordonnée par coordonnée, on peut trouver* $q_0 \in \mathcal{O}'$ *et* $\varepsilon = \dfrac{\pm 1_{\mathbb{H}} \pm I \pm J \pm K}{2} \in \mathcal{O}^\times$ *tels que* $q = 2q_0 + \varepsilon$.

    Comme $\text{dét}(\varepsilon^{-1}) = 1$, *on a alors*

$$\text{dét}(q) = \text{dét}(\varepsilon^{-1} q) = \text{dét}(2\varepsilon^{-1} q_0 + 1_{\mathbb{H}}).$$

    Or, vu la description de $\mathcal{O}^\times$, *on a* $2\varepsilon^{-1} \in \mathcal{O}'$, *donc, par stabilité par somme et produit, on a* $2\varepsilon^{-1} q_0 + 1_{\mathbb{H}} \in \mathcal{O}'$, *ce qui montre* $\text{dét}(q) \in \mathcal{S}_4$, *et conclut.*

(c) Soit p un nombre premier impair.

i. Montrer qu'il existe $a, b \in \mathbb{Z}$ l'on ait la chaîne d'inclusions strictes

$$(p\,1_{\mathbb{H}}) \subsetneq (p\,1_{\mathbb{H}}, 1_{\mathbb{H}} + a\,I + b\,J) \subsetneq \mathcal{O}.$$

D'après le lemme A (transformé en un énoncé sur les congruences), on peut trouver $a, b \in \mathbb{Z}$ *tels que* $a^2 + b^2 \equiv -1 \pmod{p}$.
On peut donc trouver un entier k *tel que* $1 + a^2 + b^2 = k\,p$, *d'où :*

$$(1_{\mathbb{H}} + a\,I + b\,J)(1_{\mathbb{H}} - a\,I - b\,J) = (1 + a^2 + b^2)1_{\mathbb{H}} = k\,p\,1_{\mathbb{H}}.$$

- *L'inclusion* $(p\,1_{\mathbb{H}}) \subseteq (p\,1_{\mathbb{H}}, 1_{\mathbb{H}} + a\,I + b\,J)$ *est claire.*
- *Si on avait l'inclusion réciproque, on aurait notamment* $1_{\mathbb{H}} + a\,I + b\,J \in (p\,1_{\mathbb{H}})$, *et on pourrait donc trouver* $\nu \in \mathcal{O}$ *tel que* $1_{\mathbb{H}} + a\,I + b\,J = \nu\,p\,1_{\mathbb{H}}$.
  On pourrait alors trouver quatre nombres $t, x, y, z \in \mathbb{R}$, *tous entiers ou tous demi-entiers, tels que* $\nu = t\,1_{\mathbb{H}} + x\,I + y\,J + z\,K$.
  L'égalité $1_{\mathbb{H}} + a\,I + b\,J = \nu\,p\,1_{\mathbb{H}}$ *donnerait alors notamment* $1 = p\,t$.
  Que t *soit entier ou demi-entier, ceci est une contradiction, car on a supposé* p *premier* ***impair***.
- *L'inclusion* $(p\,1_{\mathbb{H}}, 1_{\mathbb{H}} + a\,I + b\,J) \subseteq \mathcal{O}$ *est tautologique.*
- *Si on avait l'inclusion réciproque, on pourrait trouver* $\lambda, \mu \in \mathcal{O}$ *tels que*

$$1_{\mathbb{H}} = \lambda\,p\,1_{\mathbb{H}} + \mu\,(1_{\mathbb{H}} + a\,I + b\,J).$$

  En multipliant à droite par $1_{\mathbb{H}} - a\,I - b\,J$, *il vient :*

$$\begin{aligned} 1_{\mathbb{H}} - a\,I - b\,J &= \lambda\,p\,(1_{\mathbb{H}} - a\,I - b\,J) + \mu\,(1_{\mathbb{H}} + a\,I + b\,J)(1_{\mathbb{H}} - a\,I - b\,J) \\ &= \lambda\,p\,(1_{\mathbb{H}} - a\,I - b\,J) + \mu\,k\,p\,1_{\mathbb{H}} \\ &= p\,\underbrace{\left(\lambda\,(1_{\mathbb{H}} - a\,I - b\,J) + \mu\,k\,1_{\mathbb{H}}\right)}_{\in \mathcal{O}}. \end{aligned}$$

  Là encore, on obtient une contradiction en étudiant les premières coordonnées : on devrait avoir une égalité du type $1 = p\,t$, *pour un certain* t *entier ou demi-entier, ce qui est impossible.*

ii. En déduire qu'il existe $\gamma, \delta \in \mathcal{O}$, non inversibles, tels que $p\,1_{\mathbb{H}} = \gamma\,\delta$.

Comme $1_{\mathbb{H}} + a\,I + b\,J \neq 1_{\mathbb{H}}$*, on peut trouver* $\delta \in \mathcal{O}$ *tel que* $(p\,1_{\mathbb{H}}, 1_{\mathbb{H}} + a\,I + b\,J) = (\delta)$.
L'appartenance $p\,1_{\mathbb{H}} \in (p\,1_{\mathbb{H}}, 1_{\mathbb{H}} + a\,I + b\,J) = (\delta)$ *montre l'existence d'un élément* $\gamma \in \mathcal{O}$ *tel que* $p\,1_{\mathbb{H}} = \gamma\,\delta$.

- *Si* δ *était inversible, on aurait, pour tout* $\alpha \in \mathcal{O}$,

$$\alpha = \alpha\,\delta^{-1}\,\delta \in (\delta),$$

ce qui contredirait l'aspect strict de l'inclusion $(\delta) = (p\,1_{\mathbb{H}}, 1_{\mathbb{H}} + a\,I + b\,J) \subsetneq \mathcal{O}$.

- *Si* γ *était inversible, on aurait, pour tout* $\alpha \in \mathcal{O}$,

$$\alpha\,\delta = \alpha\,\gamma^{-1}\,\gamma\,\delta = \alpha\,p\,1_{\mathbb{H}} \in (p\,1_{\mathbb{H}}),$$

ce qui contredirait l'aspect strict de l'inclusion $(p\,1_{\mathbb{H}}) \subsetneq (p\,1_{\mathbb{H}}, 1_{\mathbb{H}} + a\,I + b\,J) = (\delta)$.

iii. En déduire enfin que $p \in \mathcal{S}_4$.

On passe l'égalité précédente au déterminant : il vient

$$p^2 = \text{dét}(p\,1_{\mathbb{H}}) = \text{dét}(\gamma)\,\text{dét}(\delta).$$

Comme γ *et* δ *ne sont pas inversibles, les entiers* $\text{dét}(\gamma)$ *et* $\text{dét}(\delta)$ *sont* $\geqslant 2$.
Comme p *est premier, la seule possibilité est* $\text{dét}(\gamma) = \text{dét}(\delta) = p$.
Ainsi, p *est la norme d'un élément* $\gamma \in \mathcal{O}$*, ce qui montre que* $p \in \mathcal{S}_4$.

(d) Montrer le *théorème des quatre carrés* : $\mathcal{S}_4 = \mathbb{N}$.

- *L'inclusion* $\mathcal{S}_4 \subseteq \mathbb{N}$ *est claire.*
- *On a vu que tout nombre premier impair appartenait à* $\mathcal{S}_4$.
  Clairement, $2 = 1^2 + 1^2 + 0^2 + 0^2 = \text{dét}(1 + I) \in \mathcal{S}_4$.
  Comme tout élément de $\mathbb{N}^*$ *s'écrit comme un produit de nombres premiers (clairement,* $0 \in \mathcal{S}_4$*) et que* $\mathcal{S}_4$ *est stable par produit, on en déduit* $\mathcal{S}_4 = \mathbb{N}$.