DM 10 : théorèmes des deux et des quatre carrés

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 $\mathbb{C}$.
2. (a) Montrer que le groupe additif $\mathbb{Z}[i]$ est engendré par la famille $(1, i)$.
   (b) Soit $\varphi : \mathbb{Z}[i] \to \mathbb{Z}[i]$ un endomorphisme d'anneaux. Montrer que $\varphi(i) = \pm i$.
   (c) En déduire que $\mathbb{Z}[i]$ possède exactement deux endomorphismes d'anneaux, et que les deux sont des automorphismes.
3. Montrer que l'application N est à valeurs dans $\mathbb{N}$ et qu'elle est *multiplicative*, c'est-à-dire que
$$\forall \alpha, \beta \in \mathbb{Z}[i], N(\alpha\,\beta) = N(\alpha)\,N(\beta).$$
4. Montrer que $\mathbb{Z}[i]^\times = \{\alpha \in \mathbb{Z}[i] \mid N(\alpha) = 1\}$ et en déduire que $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
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 $\mathbb{Z}$).
   (b) En déduire que c divise a dans $\mathbb{Z}[i]$ si et seulement si c divise a dans $\mathbb{Z}$.

- La dernière question levant toute ambiguïté, on notera simplement $\mid$ 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 $\big(\alpha \mid \beta \text{ et } \beta \mid \alpha\big) \Leftrightarrow \exists \varepsilon \in \mathbb{Z}[i]^\times : \beta = \varepsilon\,\alpha$.

- 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.
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.

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

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

(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 $5 = \pi_1 \pi_2$.

9. **Division euclidienne dans $\mathbb{Z}[i]$.**

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

(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

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

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 $(\alpha, \beta) = (\delta)$.
Indication. *On pourra considérer $\delta \in (\alpha, \beta)$ non nul, de norme minimale, et chercher à adapter la démonstration de la classification des sous-groupes de $\mathbb{Z}$.*

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 $\lambda \alpha + \mu \pi = 1$.

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

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

(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.

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.

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.

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

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 $a^2 + b^2 = -1$.

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 $\mathbb{F}_p^{\times}$.

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

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

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

       iii. Conclure 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 $\pi \mid p$.

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.
    (b) En déduire que p est un élément irréductible de $\mathbb{Z}[i]$.
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 $p \nmid n \pm i$.
    (b) En déduire que p n'est pas un élément irréductible de $\mathbb{Z}[i]$.
    (c) Montrer qu'il existe $\pi_1, \pi_2 \in \mathbb{Z}[i]$ irréductibles tels que $p = \pi_1 \pi_2$.

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 :

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

19. Montrer que l'ensemble $\mathcal{S}_2$ est stable par produit.
20. (a) En utilisant la partie III, montrer que tout nombre premier $p \equiv 1 \pmod 4$ appartient à $\mathcal{S}_2$.
    (b) En déduire que si un entier $n \in \mathbb{N}^*$ vérifie la condition $(*)$, alors $n \in \mathcal{S}_2$.
21. Soit p un nombre premier tel que $p \equiv 3 \pmod 4$ et $a, b \in \mathbb{Z}$.
    Montrer $p \mid a^2 + b^2 \Rightarrow \big(p \mid a + ib \text{ et } p \mid a - ib\big)$.
22. Conclure la démonstration du théorème des deux carrés.

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 $\quad 1_{\mathbb{H}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad$ 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 $M_2(\mathbb{C})$.
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 $q\,q^* = q^*\,q = \text{dét}(q)\,1_{\mathbb{H}}$.
    (b) L'application $q \mapsto q^*$ est-elle un endomorphisme d'anneaux de $\mathbb{H}$?
    (c) Montrer que $\mathbb{H}^\times = \mathbb{H} \setminus \{0\}$.
    (d) Peut-on en déduire que $\mathbb{H}$ est un corps ?
25. Montrer que $\mathcal{O}$ est un sous-anneau non commutatif de $\mathbb{H}$, et montrer que $\forall q \in \mathcal{O}, \text{dét}(q) \in \mathbb{N}$.
26. Montrer que $\mathcal{O}^\times = \{q \in \mathcal{O} \mid \text{dét}(q) = 1\}$ et déterminer exactement les éléments de $\mathcal{O}^\times$.
27. **Arithmétique dans $\mathcal{O}$.**
    (a) Montrer que $\forall z \in \mathbb{H}, \exists \kappa \in \mathcal{O} : \text{dét}(\kappa - z) < 1$.
    (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

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

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 $\underbrace{\{\lambda\,\alpha + \mu\,\beta \mid \lambda, \mu \in \mathcal{O}\}}_{(\alpha,\beta)} = \underbrace{\{\nu\,\delta \mid \nu \in \mathcal{O}\}}_{(\delta)}$. On ne demande pas de le vérifier.

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.
    (b) Montrer que $\mathcal{S}_4 = \{\text{dét}(q) \mid q \in \mathcal{O}\}$.
    Indication. *On pourra utiliser* $\text{dét}(q) = \text{dét}(\varepsilon\,q)$, *pour une unité* $\varepsilon \in \mathcal{O}^\times$ *bien choisie.*
    (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

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

        ii. En déduire qu'il existe $\gamma, \delta \in \mathcal{O}$, non inversibles, tels que $p\,1_{\mathbb{H}} = \gamma\,\delta$.
        iii. En déduire enfin que $p \in \mathcal{S}_4$.
    (d) Montrer le *théorème des quatre carrés* : $\mathcal{S}_4 = \mathbb{N}$.

Bonnes vacances, et bonne année $15^2 + 22^2 + 23^2 + 28^2$ *à tous !*
