ARITHMÉTIQUE DES ENTIERS DE GAUSS

On s'intéresse dans ce devoir à l'ensemble : $\mathbb{Z}[\mathrm{i}] = \left\{a + \mathrm{i}b \mid \quad a, b \in \mathbb{Z}\right\}$ des *entiers de Gauss*. Il a été démontré en TD que $\mathbb{Z}[\mathrm{i}]$ est un sous-anneau de $\mathbb{C}$, que pour tout $x \in \mathbb{Z}[\mathrm{i}]$: $|x|^2 \in \mathbb{N}$ et que : $\mathrm{U}\big(\mathbb{Z}[\mathrm{i}]\big) = \big\{\pm 1, \pm \mathrm{i}\big\} = \left\{z \in \mathbb{Z}[\mathrm{i}] \mid \quad |z|^2 = 1\right\}$.

L'appellation *entier de Gauss* ne peut que paraître douteuse quand on n'a jamais envisagé la notion d'entier au-delà du monde $\mathbb{Z}$. Vous comprendrez mieux après ce devoir, en principe, en quoi les structures algébriques sont riches de sens en dépit de leur apparente gratuité et susceptibles de révéler de nombreux phénomènes mathématiques qui resteraient cachés sans. Vous aussi, vous vous direz alors : « Mais oui, ce sont des entiers ! »

Le vocabulaire de l'arithmétique dans $\mathbb{Z}$ peut d'ailleurs être importé facilement dans l'anneau $\mathbb{Z}[\mathrm{i}]$. Prenez bien garde cependant de ne pas confondre une idée que vous avez dans $\mathbb{Z}$ et une idée que vous avez dans $\mathbb{Z}[\mathrm{i}]$. Les mots coïncident, mais pas les objets. Sauf précision contraire, on mène dans ce devoir des raisonnements dans $\mathbb{Z}[\mathrm{i}]$.

Définition **(Divisibilité et association dans $\mathbb{Z}[\mathrm{i}]$)** Soient $x, y \in \mathbb{Z}[\mathrm{i}]$.

- On dit que x *divise* y ou que x est un *diviseur de* y s'il existe un élément $k \in \mathbb{Z}[\mathrm{i}]$ pour lequel : $y = kx$.
- On dit que y est *associé à* x s'il existe un élément $u \in \mathrm{U}\big(\mathbb{Z}[\mathrm{i}]\big)$ pour lequel : $y = ux$.

1) a) Justifier l'assertion suivante : « $\mathrm{U}\big(\mathbb{Z}[\mathrm{i}]\big)$ est un groupe, donc la relation d'association est une relation d'équivalence sur $\mathbb{Z}[\mathrm{i}]$. »

b) Montrer que pour tous $x, y \in \mathbb{Z}[\mathrm{i}]$, x et y sont associés si et seulement si x et y se divisent mutuellement.

2) a) Montrer que pour tous $x, y \in \mathbb{Z}[\mathrm{i}]$ avec : $y \neq 0$, il existe un couple $(q, r) \in \mathbb{Z}[\mathrm{i}]^2$ pour lequel : $x = qy + r$ et $|r|^2 < |y|^2$ — *théorème de la division euclidienne*. On pourra approximer $\dfrac{x}{y}$ par un élément de $\mathbb{Z}[\mathrm{i}]$.

b) Montrer que le couple (q, r) de la question **a)** n'est pas forcément unique.

Définition **(Couple d'éléments premiers entre eux dans $\mathbb{Z}[\mathrm{i}]$)** Soient $x, y \in \mathbb{Z}[\mathrm{i}]$. On dit que x et y sont *premiers entre eux* si leurs seuls diviseurs communs sont les éléments de $\mathrm{U}\big(\mathbb{Z}[\mathrm{i}]\big)$.

3) Soient $x, y \in \mathbb{Z}[\mathrm{i}]$ premiers entre eux. On pose : $\mathbb{Z}[\mathrm{i}]x + \mathbb{Z}[\mathrm{i}]y = \left\{ux + vy \mid \quad u, v \in \mathbb{Z}[\mathrm{i}]\right\}$.

a) Montrer que l'ensemble $\left\{|z|^2 \mid \quad z \in \mathbb{Z}[\mathrm{i}]x + \mathbb{Z}[\mathrm{i}]y \quad \text{et} \quad z \neq 0\right\}$ possède un plus petit élément m.

On peut dès lors se donner un élément $d \in \mathbb{Z}[\mathrm{i}]x + \mathbb{Z}[\mathrm{i}]y$ non nul pour lequel : $|d|^2 = m$.

b) Montrer que d divise x.

c) En déduire l'existence de deux éléments $u, v \in \mathbb{Z}[\mathrm{i}]$ pour lesquels : $ux + vy = 1$ — *théorème de Bézout*.

4) Soient $x, y, z \in \mathbb{Z}[\mathrm{i}]$. On suppose que x divise yz et que x et y sont premiers entre eux. Montrer qu'alors x divise z — *théorème de Gauss*.

Définition **(Irréductibles de $\mathbb{Z}[\mathrm{i}]$)** Soit $x \in \mathbb{Z}[\mathrm{i}]$. On dit que x est *irréductible* si x n'est pas inversible et si ses seuls diviseurs sont 1, x et leurs associés.

On se donne à présent arbitrairement un *ensemble P de représentants des classes d'équivalence des irréductibles de $\mathbb{Z}[\mathrm{i}]$ pour la relation d'association*. Cette expression signifie que P est une partie de $\mathbb{Z}[\mathrm{i}]$ satisfaisant les trois conditions suivantes :

— tout élément de P est irréductible,

— tout irréductible de $\mathbb{Z}[\mathrm{i}]$ est associé à un élement de P,

— les éléments de P sont deux à deux non associés.

5) Montrer que pour tout $x \in \mathbb{Z}[\mathrm{i}]$ non nul, il existe un élément $u \in \mathrm{U}\big(\mathbb{Z}[\mathrm{i}]\big)$ et une famille presque nulle $(\alpha_p)_{p\in P}$ d'entiers naturels pour lesquels : $x = u\prod_{p\in P} p^{\alpha_p}$ — existence d'une *factorisation irréductible*.

On **ADMET** maintenant le résultat suivant, dont la preuve ressemble cela dit à s'y méprendre à celle qu'on a proposée dans $\mathbb{Z}$.

Définition-théorème (Valuation p-adique et unicité de la factorisation irréductible)

- Soit $p \in P$. L'ensemble $\Big\{n \in \mathbb{N} \mid \quad p^n \text{ divise } x\Big\}$ possède un plus grand élément pour tout $x \in \mathbb{Z}[\mathrm{i}]$ non nul, appelé la *valuation p-adique de x* et noté $v_p(x)$.

  Pour tous $x, y \in \mathbb{Z}[\mathrm{i}]$ non nuls : $v_p(xy) = v_p(x) + v_p(y)$.
- La factorisation irréductible est unique dans $\mathbb{Z}[\mathrm{i}]$ à l'ordre des facteurs près.

6) Montrer que pour tous $x, y \in \mathbb{Z}[\mathrm{i}]$ premiers entre eux, si xy est le cube d'un élément de $\mathbb{Z}[\mathrm{i}]$, x et y en sont aussi.

En guise d'application des résultats qui précèdent, on s'intéresse maintenant à l'*équation de Mordell* : $y^2 = x^3 - 1$ d'inconnue $(x, y) \in \mathbb{Z}^2$. Plus généralement, les *équations de Mordell* sont les équations diophantiennes de la forme : $y^2 = x^3 + k$ d'inconnue $(x, y) \in \mathbb{Z}^2$ dans lesquelles $k \in \mathbb{Z}$ est fixé.

7) Soit $(x, y) \in \mathbb{Z}^2$. On suppose que : $y^2 = x^3 - 1$. Soit $d \in \mathbb{Z}[\mathrm{i}]$ un diviseur commun de $y + \mathrm{i}$ et $y - \mathrm{i}$.

a) Montrer que dans $\mathbb{Z}$, $|d|^2$ divise à la fois 4 et x^3.

b) Montrer que x est impair en raisonnant modulo 4.

c) En déduire que : $d \in \mathrm{U}\big(\mathbb{Z}[\mathrm{i}]\big)$.

8) Montrer finalement que la seule solution de l'équation de Mordell : $y^2 = x^3 - 1$ d'inconnue $(x, y) \in \mathbb{Z}^2$ est le couple $(1, 0)$.

Les questions qui suivent sont facultatives.

9) Montrer que pour tout $p \in \mathbb{P}$ impair, si p est la somme de deux carrés d'entiers, alors : $p \equiv 1\ [4]$.

À présent, soit $p \in \mathbb{P}$ impair. On suppose : $p \equiv 1\ [4]$. On a vu en TD dans le chapitre « Arithmétique des entiers relatifs » qu'en posant : $a = \left(\frac{p-1}{2}\right)!$, alors : $a^2 \equiv -1\ [p]$.

10) a) Montrer que p et $a + \mathrm{i}$ ne sont pas premiers entre eux.

On peut donc se donner un diviseur commun $d \in \mathbb{Z}[\mathrm{i}]$ de p et $a + \mathrm{i}$ qui n'appartient pas à $\mathrm{U}\big(\mathbb{Z}[\mathrm{i}]\big)$.

b) Que peut valoir $|d|^2$?

c) Montrer que l'hypothèse : $|d|^2 = p^2$ conduit à une contradiction.

d) En déduire que p est la somme de deux carrés d'entiers.

On a finalement atteint grâce aux entiers de Gauss — notamment — le résultat que voici.

Théorème (Théorème des deux carrés) Pour tout $p \in \mathbb{P}$ impair, p est la somme de deux carrés d'entiers si et seulement si : $p \equiv 1\ [4]$.