LES ENTIERS D'EISENSTEIN

On appelle *entier d'Eisenstein* tout nombre complexe de la forme $a+\mathrm{j}b$ avec $a,b\in\mathbb{Z}$ et on note $\mathbb{Z}[\mathrm{j}]$ leur ensemble. Commencez peut-être par vous remémorer toutes les relations que vous êtes censés connaître sur le nombre j…

1) Montrer que $\mathbb{Z}[\mathrm{j}]$, muni de la multiplication et de l'addition des nombres complexes, est un anneau commutatif.

2) Pour tout $z\in\mathbb{Z}[\mathrm{j}]$, on appelle *norme de* z et on note $N(z)$ le nombre $z\overline{z}$.

a) Montrer que pour tous $z,z'\in\mathbb{Z}[\mathrm{j}]$: $\quad\overline{z}\in\mathbb{Z}[\mathrm{j}],\quad N(z)\in\mathbb{N}\quad$ et $\quad N(zz')=N(z)N(z')$.

b) Montrer l'égalité : $\quad\mathrm{U}\big(\mathbb{Z}[\mathrm{j}]\big)=\Big\{z\in\mathbb{Z}[\mathrm{j}]\ |\quad N(z)=1\Big\}$.

c) En déduire que : $\quad\mathrm{U}\big(\mathbb{Z}[\mathrm{j}]\big)=\mathbb{U}_6$.

L'appellation *entier d'Eisenstein* 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 $\mathbb{Z}$ est facile à importer dans l'anneau $\mathbb{Z}[\mathrm{j}]$. Prenez bien garde cependant de ne pas confondre une idée que vous avez dans $\mathbb{Z}$ et une idée que vous avez dans $\mathbb{Z}[\mathrm{j}]$. Les mots coïncident, mais pas les objets. On mène dans ce devoir des raisonnements dans $\mathbb{Z}[\mathrm{j}]$, sauf quand il est explicitement précisé qu'on travaille dans $\mathbb{Z}$.

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

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

3) **a)** Montrer que la relation d'association est une relation d'équivalence sur $\mathbb{Z}[\mathrm{j}]$.

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

4) **a)** Montrer que tout nombre complexe peut être écrit $x+\mathrm{j}y$ pour certains $x,y\in\mathbb{R}$ et vérifier que pour tous $x,y\in\mathbb{R}$: $|x+\mathrm{j}y|^2\leqslant x^2+|xy|+y^2$.

b) En déduire que tout nombre complexe est à distance au plus $\dfrac{\sqrt{3}}{2}$ d'un élément de $\mathbb{Z}[\mathrm{j}]$.

c) En déduire que pour tous $x,y\in\mathbb{Z}[\mathrm{j}]$ avec : $\quad y\neq 0,\quad$ il existe un couple $(q,r)\in\mathbb{Z}[\mathrm{j}]^2$ pour lequel : $\quad x=qy+r$ et $\quad N(r)<N(y)\quad$ (*théorème de la division euclidienne*).

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

5) Soient $x,y\in\mathbb{Z}[\mathrm{j}]$ premiers entre eux. On pose : $\quad\mathbb{Z}[\mathrm{j}]x+\mathbb{Z}[\mathrm{j}]y=\Big\{ux+vy\ |\quad u,v\in\mathbb{Z}[\mathrm{j}]\Big\}$.

a) Montrer que l'ensemble $\Big\{N(z)\ |\quad z\in\mathbb{Z}[\mathrm{j}]x+\mathbb{Z}[\mathrm{j}]y\quad\text{et}\quad z\neq 0\Big\}$ possède un plus petit élément m.

On peut dès lors se donner un élément $d\in\mathbb{Z}[\mathrm{j}]x+\mathbb{Z}[\mathrm{j}]y$ non nul pour lequel : $\quad N(d)=m$.

b) Montrer que d divise x.

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

On ADMET à présent quelques résultats supplémentaires « bien connus » dont les preuves dans $\mathbb{Z}[\mathrm{j}]$ ressemblent à s'y méprendre à leurs analogues dans $\mathbb{Z}$.

Théorème **(Théorème de Gauss)** Soient $x,y,z\in\mathbb{Z}[\mathrm{j}]$. Si x divise yz et si x et y sont premiers entre eux, alors x divise z.

Définition (Irréductibles de $\mathbb{Z}[\mathrm{j}]$) Soit $x \in \mathbb{Z}[\mathrm{j}]$. 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 $\mathbb{Z}[\mathrm{j}]$ pour la relation d'association*. Cette expression signifie que P est une partie de $\mathbb{Z}[\mathrm{j}]$ satisfaisant les trois conditions suivantes :

— tout élément de P est irréductible,

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

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

Définition-théorème (Valuation p-adique et factorisation irréductible)

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

  Pour tous $x, y \in \mathbb{Z}[\mathrm{j}]$ non nuls : $\quad v_p(xy) = v_p(x) + v_p(y)$.

- **Factorisation irréductible :** Pour tout $x \in \mathbb{Z}[\mathrm{j}]$ non nul, il existe un et un seul élément $u \in \mathrm{U}\big(\mathbb{Z}[\mathrm{j}]\big)$ et une et une seule famille presque nulle $(\alpha_p)_{p\in P}$ d'entiers naturels pour lesquels : $\quad x = u\prod_{p\in P} p^{\alpha_p}$. En l'occurrence, pour tout $p \in P$: $\quad \alpha_p = v_p(x)$.

En guise d'application des résultats qui précèdent, on s'intéresse à présent à une caractérisation des nombres premiers congrus à 1 modulo 3. L'équivalence des assertions (i) et (ii) a été démontrée par Euler en 1759.

Théorème (Nombres premiers congrus à 1 modulo 3) Soit p un nombre premier supérieur ou égal à 5. Les assertions suivantes sont équivalentes :

(i) $\quad p \equiv 1\ [3]$.

(ii) $\quad p = x^2 + 3y^2 \quad$ pour certains $x, y \in \mathbb{N}$.

(iii) -3 est un carré modulo p, i.e : $\quad -3 \equiv n^2\ [p] \quad$ pour un certain $n \in \mathbb{Z}$.

Dans les questions qui suivent, p est un nombre premier supérieur ou égal à 5 fixé.

6) Montrer l'implication (ii) $\Longrightarrow$ (i).

7) On démontre dans cette question l'implication (iii) $\Longrightarrow$ (ii). On fait l'hypothèse que -3 est un carré modulo p, i.e. que pour certains $n, q \in \mathbb{Z}$: $\quad n^2 + 3 = pq$.

a) Montrer que $\dfrac{n+\mathrm{i}\sqrt{3}}{p}$ et $\dfrac{n-\mathrm{i}\sqrt{3}}{p}$ ne sont pas des entiers d'Eisenstein.

b) En déduire que pour un certain $z \in \mathbb{Z}[\mathrm{j}]$: $\quad N(z) = p$.

c) Montrer que l'un des entiers d'Eisenstein z, $\mathrm{j}z$ et $\mathrm{j}^2 z$ est de la forme $x + \mathrm{i}y\sqrt{3}$ avec $x, y \in \mathbb{Z}$, puis conclure.

8) Cette dernière question est facultative. On y démontre l'équivalence des assertions (i) et (iii). On travaille pour ce faire dans l'anneau $\dfrac{\mathbb{Z}}{p\mathbb{Z}} = \left\{\overline{0}, \overline{1}, \ldots, \overline{p-1}\right\}$, dont on rappelle que c'est un corps car p est premier.

On note E l'ensemble $\dfrac{\mathbb{Z}}{p\mathbb{Z}} \setminus \left\{\overline{0}, \overline{1}\right\}$, φ l'application $x \longmapsto \overline{1} - \dfrac{\overline{1}}{x}$ sur E et F l'ensemble des points fixes de φ.

a) Montrer que φ est bijective de E sur E et que : $\quad \varphi^3 = \mathrm{Id}_E \quad$ où : $\quad \varphi^3 = \varphi \circ \varphi \circ \varphi$.

On définit à présent une relation binaire $\sim$ sur E de la façon suivante — pour tous $x, y \in E$:

$$x \sim y \qquad \Longleftrightarrow \qquad \exists\, k \in \mathbb{Z}, \quad y = \varphi^k(x).$$

b) Montrer que $\sim$ est une relation d'équivalence sur E.

c) Étudier le cardinal des classes d'équivalence de $\sim$, puis montrer que : $\quad |E| \equiv |F|\ [3]$.

d) Montrer que F est vide si -3 n'est pas un carré modulo p et de cardinal 2 sinon.

e) Conclure.