Entiers d'Eisenstein

Trois niveaux de difficulté/longueur :

— Piste bleue : partie **1**.

— Piste rouge : parties **1** et **2**.

— Piste noire : tout le devoir. La partie **3** est particulièrement subtile. Je vous encourage à la chercher, mais je ne veux pas la corriger !

1 Arithmétique de l'anneau $\mathbb{Z}[\mathrm{j}]$

On appelle *entier d'Eisenstein* tout nombre complexe $a+\mathrm{j}b$ 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 le réel positif $N(z)=|z|^2=z\overline{z}$.

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 que $\mathrm{U}\big(\mathbb{Z}[\mathrm{j}]\big)=\Big\{z\in\mathbb{Z}[\mathrm{j}]\ |\quad N(z)=1\Big\}=\mathbb{U}_6$.

L'appellation *entier d'Eisenstein* peut sembler abusive, mais vous comprendrez mieux après ce devoir en quoi les structures algébriques révèlent des phénomènes profonds qui resteraient cachés sans.

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 éléments associés 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 si $y=kx$ pour un certain $k\in\mathbb{Z}[\mathrm{j}]$.
- On dit que y est *associé à* x si $y=ux$ pour un certain $u\in\mathrm{U}\big(\mathbb{Z}[\mathrm{j}]\big)$.

3) a) Justifier l'assertion « $\mathrm{U}\big(\mathbb{Z}[\mathrm{j}]\big)$ est un groupe, donc 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 : $\quad\forall z\in\mathbb{C},\quad\exists!\,(a,b)\in\mathbb{R},\quad z=a+\mathrm{j}b$.

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 $x\in\mathbb{Z}[\mathrm{j}]$ et $y\in\mathbb{Z}[\mathrm{j}]^*$, il existe un couple $(q,r)\in\mathbb{Z}[\mathrm{j}]^2$ pour lequel $x=qy+r$ et $N(r)<N(y)$ (*théorème de la division euclidienne*).

Définition (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.

a) Montrer que l'ensemble $N\Big(\big(\mathbb{Z}[\mathrm{j}]\,x+\mathbb{Z}[\mathrm{j}]\,y\big)\smallsetminus\{0\}\Big)$ possède un plus petit élément m.

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

b) Montrer que d divise x et y, puis que $ux+vy=1$ pour certains $u,v\in\mathbb{Z}[\mathrm{j}]$ (*théorème de Bézout*).

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

6) Soient $p \in \mathbb{Z}[\mathrm{j}]$ irréductible et $x, y \in \mathbb{Z}[\mathrm{j}]$. Montrer que p divise xy si et seulement si p divise x ou y (*lemme d'Euclide*).

Il n'est pas dur de montrer que les associés d'un irréductible sont eux-mêmes irréductibles. On se donne à présent arbitrairement un ensemble quelconque P de représentants des classes d'équivalence d'irréductibles de $\mathbb{Z}[\mathrm{j}]$ pour la relation d'association. En d'autres termes, 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 élément de P,

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

7) Montrer que pour tout $x \in \mathbb{Z}[\mathrm{j}]^*$, il existe un élément $u \in \mathrm{U}(\mathbb{Z}[\mathrm{j}])$ et une famille presque nulle $(\alpha_p)_{p\in P}$ d'entiers naturels pour lesquels $x = u \prod_{p\in P} p^{\alpha_p}$. Cette relation est appelée une *factorisation irréductible de x*.

On admet finalement les résultats suivants, qui se démontrent comme leurs analogues dans $\mathbb{Z}$.

Définition-théorème **(Valuation p-adique et unicité de la factorisation irréductible dans $\mathbb{Z}[\mathrm{j}]$)**

- Soit $p \in P$. L'ensemble $\left\{n \in \mathbb{N} \mid \ p^n \text{ divise } x\right\}$ possède un plus grand élément pour tout $x \in \mathbb{Z}[\mathrm{j}]^*$, appelé la *valuation p-adique de x* et noté $v_p(x)$. En outre, pour tous $x, y \in \mathbb{Z}[\mathrm{j}]^*$: $\quad v_p(xy) = v_p(x) + v_p(y)$.
- La factorisation irréductible d'un élément de $\mathbb{Z}[\mathrm{j}]$ est unique à l'ordre près des facteurs.

2 Nombres premiers de la forme $x^2 + 3y^2$

On démontre dans cette partie la caractérisation suivante.

Théorème **(Nombres premiers de la forme x^2+3y^2)** Soit $p \in \mathbb{P} \smallsetminus \{2, 3\}$. Les assertions suivantes sont équivalentes :

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

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

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

L'équivalence des assertions (i) et (ii) a été démontrée par le mathématicien suisse Leonhard Euler (1707-1783) en 1759.

Dans les questions **8)** à **10)**, p est un nombre premier fixé distinct de 2 et 3.

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

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

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, puis que $N(z) = p$ pour un certain $z \in \mathbb{Z}[\mathrm{j}]$.

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

10) Pour prouver l'équivalence des assertions (i) et (iii), on travaille dans le corps $\mathbb{F}_p$, dont les éléments seront notés $0, \ldots, p-1$ plutôt que $\overline{0}, \ldots, \overline{p-1}$ par souci de légèreté.

On note f l'application $x \longmapsto 1 - x^{-1}$ sur $E = \mathbb{F}_p \smallsetminus \{0, 1\}$ et F l'ensemble de ses points fixes. Pour tous $x, y \in E$, on dit enfin que $x \sim y$ si $y = f^k(x)$ pour un certain $k \in \mathbb{Z}$.

a) Montrer que f est une permutation de E et que $f^3 = \mathrm{Id}_E$ où $f^3 = f \circ f \circ f$.

b) Montrer que $\sim$ est une relation d'équivalence sur E, puis que $|F| \equiv p - 2\ [3]$.

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

3 Équation de Fermat $x^3 + y^3 = z^3$

On prouve dans cette partie que l'*équation de Fermat* $x^3 + y^3 = z^3$ d'inconnue $(x, y, z) \in (\mathbb{Z}^*)^3$ n'a pas de solution. Comme $(-1)^3 = -1$, il est équivalent de dire que l'équation plus symétrique $x^3 + y^3 + z^3 = 0$ n'a pas de solution dans $(\mathbb{Z}^*)^3$.

Raisonnant par l'absurde, on suppose l'existence d'un triplet $(x, y, z) \in (\mathbb{Z}^*)^3$ pour lequel $x^3 + y^3 + z^3 = 0$. On le choisit sans perte de généralité de telle sorte que le produit $|xyz|$ soit minimal.

On admet, pour l'avoir déjà démontré, que si un produit d'entiers premiers entre eux deux à deux dans $\mathbb{Z}$ est le cube d'un entier, alors chacun de ces entiers est lui-même le cube d'un entier.

11) Montrer que x, y et z sont premiers entre eux dans $\mathbb{Z}$ et qu'on peut supposer x et y impairs sans perte de généralité.

Sur une idée d'Euler, on pose alors $m = \dfrac{x+y}{2}$ et $n = \dfrac{x-y}{2}$, qui appartiennent à $\mathbb{Z}$ d'après **11)**.

12) Dans cette question, on fait de l'arithmétique seulement dans $\mathbb{Z}$ et non dans $\mathbb{Z}[\mathrm{j}]$.

a) Vérifier que $2m\left(m^2 + 3n^2\right) = (-z)^3$ et montrer que m et n sont premiers entre eux de parités différentes.

b) Montrer que $(2m) \wedge \left(m^2 + 3n^2\right) \in \{1, 3\}$ et en déduire dans les deux cas une égalité de la forme $r^2 + 3s^2 = t^3$ où les entiers r, s et t possèdent les propriétés suivantes :

— r et s sont premiers entre eux de parités différentes,

— $2r$ est le cube d'un entier et $0 < 2|r| \leqslant |x+y|$, ou bien $\dfrac{2s}{3}$ est le cube d'un entier et $0 < \dfrac{2|s|}{3} \leqslant |x+y|$.

c) Montrer que $|x + y| \leqslant |xyz|^3$.

13) a) Montrer que $r + \mathrm{i}s\sqrt{3}$ et $r + \mathrm{i}s\sqrt{3}$ appartiennent à $\mathbb{Z}[\mathrm{j}]$.

Soit d un diviseur commun de $r + \mathrm{i}s\sqrt{3}$ et $r - \mathrm{i}s\sqrt{3}$.

b) Montrer que $N(d)$ est impair et divise $4r^2$ et $12s^2$ dans $\mathbb{Z}$, puis que $r + \mathrm{i}s\sqrt{3}$ et $r - \mathrm{i}s\sqrt{3}$ sont premiers entre eux.

Cette fois, un raisonnement sur les valuations p-adiques dans $\mathbb{Z}[\mathrm{j}]$ dans la relation $\left(r + \mathrm{i}s\sqrt{3}\right)\left(r + \mathrm{i}s\sqrt{3}\right) = t^3$ montre que $r + \mathrm{i}s\sqrt{3} = u(a + \mathrm{j}b)^3$ pour certains $u \in \mathrm{U}\left(\mathbb{Z}[\mathrm{j}]\right)$ et $a, b \in \mathbb{Z}$.

c) Montrer qu'on peut choisir u dans $\mathbb{U}_3$.

14) a) Montrer que si $u = \mathrm{j}$, alors $r + s = 3ab(b - a)$, puis dénicher une contradiction modulo 2.

Un raisonnement analogue exclut le cas $u = \mathrm{j}^2$, donc $u = 1$. Un calcul sans grand intérêt montre ensuite que :

$$2r = (a - 2b)(2a - b)(a + b) \qquad \text{et} \qquad \frac{2s}{3} = ab(a - b).$$

b) Montrer que a, b et $a - b$ sont premiers entre eux deux à deux dans $\mathbb{Z}$.

On montre de même que $a - 2b$, $2a - b$ et $a + b$ sont premiers entre eux deux à deux dans $\mathbb{Z}$.

c) Observer que $(a - 2b) + (b - 2a) + (a + b) = 0$ et $(-a) + b + (a - b) = 0$, puis conclure.