Exercices d'algèbre – Fiche 7: Entiers de Gauss

Responsable: Isar Stubbe

---

1. Vérifier que l'ensemble $\mathbb{Z}[\sqrt{-3}] = \{m + n\sqrt{-3} \mid m, n \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$ contenant l'anneau $\mathbb{Z}$. On va montrer que $\mathbb{Z}[\sqrt{-3}]$ n'est pas à factorisation unique (et donc pas non plus principal ou euclidien). Dans la suite on note $N(z) = z\overline{z}$ pour la *norme* de $z \in \mathbb{C}$.
   (a) Vérifier que $N(z_1 z_2) = N(z_1)N(z_2)$ pour tout $z_1, z_2 \in \mathbb{C}$.
   (b) En déduire les éléments inversibles de $\mathbb{Z}[\sqrt{-3}]$.
   (c) Trouver deux factorisations ("non-associées") de 4 dans $\mathbb{Z}[\sqrt{-3}]$.
   (d) Montrer que 2 est irréductible mais pas premier dans $\mathbb{Z}[\sqrt{-3}]$.

2. Vérifier que l'ensemble $\mathbb{Z}[i] = \{m + ni \mid m, n \in \mathbb{Z}\}$ des *entiers de Gauss* est un sous-anneau de $\mathbb{C}$ contenant $\mathbb{Z}$. On va montrer que cet anneau est euclidien pour la norme $N(z) = z\overline{z}$. Pour $a, b \in \mathbb{Z}[i]$ avec $b \neq 0$, on calcule $z = \frac{a}{b}$ dans $\mathbb{C}$. Soit $z = x + yi$ avec $x, y \in \mathbb{R}$, et notons $m \in \mathbb{Z}$ l'arrondi entier de x, et $n \in \mathbb{Z}$ l'arrondi entier de y. (Faire un dessin dans le plan complexe pour montrer que $m + ni$ est l'entier de Gauss "le plus près" de $x + yi$.)
   (a) Observer que $|x - m| \leq \frac{1}{2}$ et $|y - n| \leq \frac{1}{2}$.
   (b) En déduire que $N\Big(b((x - m) + (y - n)i)\Big) < N(b)$.
   (c) Poser $q = m + ni$, $r = a - bq$, et conclure.
   (d) Diviser (avec reste) $15 + 9i$ par $2 - i$ dans $\mathbb{Z}[i]$.

   On va déterminer les éléments irréductibles de $\mathbb{Z}[i]$. Puisque *irréductible* est synonyme de *premier* dans cet anneau (pourquoi?), on parle de *nombres premiers de Gauss*.
   (e) Déterminer les éléments inversibles de $\mathbb{Z}[i]$.
   (f) En déduire que, si z divise $z' \neq 0$ dans $\mathbb{Z}[i]$, alors z est un diviseur propre si et seulement si $1 < N(z) < N(z')$.
   (g) Montrer que, si z est premier dans $\mathbb{Z}[i]$, alors aussi $\overline{z}$ l'est. Conclure que, dans le plan complexe, les nombres premiers de Gauss présentent une symétrie *par octant*: l'axe réelle, l'axe imaginaire, et leur deux bissectrices, sont des axes de symétrie.
   (h) Montrer que toute somme de carrés d'entiers est un produit dans $\mathbb{Z}[i]$.
   (i) Soit $p = m^2 + n^2 \in \mathbb{Z}$ un nombre premier qui est une somme de carrés non-nuls ($2 = 1^2 + 1^2$, $5 = 1^2 + 2^2$, $17 = 1^2 + 4^2$, ...). Montrer que p n'est pas premier dans $\mathbb{Z}[i]$, mais que $m + ni$ l'est (avec $m \neq 0 \neq n$ donc).
   Indication. $N(m + ni) = p$ n'a pas de diviseurs propres dans $\mathbb{N}$.
   (j) Soit $z = m + in$ un élément premier dans $\mathbb{Z}[i]$, avec $m \neq 0 \neq n$. Montrer que $N(z)$ est premier dans $\mathbb{Z}$ (et donc une somme de deux carrés non-nuls).
   Indication. Si $N(z) = rs$ dans $\mathbb{N}$, alors les facteurs premiers de r et s dans $\mathbb{Z}[i]$ donnent des facteurs premiers de $N(z)$ dans $\mathbb{Z}[i]$. Mais $N(z) = z\overline{z}$ est déja une factorisation en facteurs premiers dans $\mathbb{Z}[i]$. Conclure par l'unicité d'une telle factorisation.
   (k) Soit $p \in \mathbb{Z}$ un nombre premier qui n'est pas somme de deux carrés non-nuls (3, 7, 11, ...). Montrer que p est aussi premier dans $\mathbb{Z}[i]$.
   Indication. Si $z = m + ni$ est un diviseur propre de p dans $\mathbb{Z}[i]$, alors $N(z) = m^2 + n^2$ divise $N(p) = p^2$ dans $\mathbb{N}$, et $1 < N(z) < p^2$.
   (l) Finalement, montrer aussi: si $p \in \mathbb{Z}$ est premier dans $\mathbb{Z}[i]$, alors p est premier dans $\mathbb{Z}$ (et n'est pas une somme de carrés non-nuls).