Les entiers de Gauss : $\mathbb{Z}[i]$

Parimaths, 23 novembre 2013

Définition
On définit l'ensemble des *entiers de Gauss* comme l'ensemble

$$\mathbb{Z}[i] := \{a + bi,\ a, b \in \mathbb{Z}\},$$

où i représente la racine carrée de -1.

Problème 1 : L'anneau commutatif $\mathbb{Z}[i]$
On dit qu'un ensemble A est un anneau lorsqu'il admet deux lois de composition "$+$" et "$\cdot$" (appelées addition et multiplication) vérifiant les propriétés suivantes :

- L'addition est associative : $\forall\, a, b, c \in A,\ (a + b) + c = a + (b + c)$.
- L'addition est commutative : $\forall\, a, b \in A,\ a + b = b + a$.
- L'addition admet un neutre (noté 0) : $\forall\, a \in A,\ a + 0 = a$.
- L'addition admet un inverse : $\forall\, a \in A,\ \exists a' \in A,\ a + a' = 0$.
- La multiplication est associative.
- La multiplication est distributive par rapport à l'addition :
  $\forall\, a, b, c \in A,\ a \cdot (b + c) = a \cdot b + a \cdot c,\ (b + c) \cdot a = b \cdot a + c \cdot a$.

Si la multiplication est de plus commutative, on dit que l'anneau A est commutatif. Montrer que $\mathbb{Z}[i]$ est un tel anneau.

Problème 2 : Définition d'un nombre premier
On sait qu'un nombre $n \in \mathbb{N}$ est dit premier si et seulement s'il admet *exactement* deux diviseurs, à savoir 1 et lui-même. Que faut-il changer dans cette définition pour qu'elle ait un sens dans $\mathbb{Z}$? et dans $\mathbb{Z}[i]$? Peut-on alors donner une définition du pgcd sur $\mathbb{Z}$ et sur $\mathbb{Z}[i]$?

Essayez de reénoncer (et de démontrer !) le théorème fondamental de l'arithmétique pour l'anneau $\mathbb{Z}$. Aura-t-on la même chose sur $\mathbb{Z}[i]$? (cf. le problème 5 pour la réponse)

Problème 3 : L'anneau euclidien $\mathbb{Z}[i]$
Un anneau A est dit *euclidien* s'il existe une fonction $f : A \setminus \{0\} \to \mathbb{N}$ telle que, pour toute paire d'éléments $a, b \in A$, il existe une deuxième paire $q, r \in A$ telle que

$$a = q \cdot b + r \quad \text{et soit} \quad r = 0 \quad \text{ou bien} \quad f(r) < f(b).$$

Démontrer que $\mathbb{Z}$ est un anneau euclidien. Quelle est sa fonction f ? En faire de même avec $\mathbb{Z}[i]$. Montrer par ailleurs que, pour tout $n \in \mathbb{N}$, il n'existe qu'une quantité finie d'entiers de Gauss $x \in \mathbb{Z}[i]$ tels que $f(x) \leq n$.

Problème 4 : Quelques théorèmes sur $\mathbb{Z}[i]$
Démontrez le théorème de Bézout, puis le lemme de Gauss pour $\mathbb{Z}[i]$. Ce sont les énoncés suivants :

Théorème 1 (Bézout)**.** *Soient $a, b \in \mathbb{Z}[i]$ des entiers de Gauss premiers entre eux (i.e.* $\text{pgcd}(a, b) = 1$*), alors il existe des entiers de Gauss $u, v \in \mathbb{Z}[i]$ tels que*

$$au + bv = 1.$$

Théorème 2 (Lemme de Gauss)**.** *Soit q un "premier de Gauss" (i.e. un nombre premier dans $\mathbb{Z}[i]$). Alors, pour $a, b \in \mathbb{Z}[i]$ on a*

$$q | ab \Rightarrow q | a \text{ ou } q | b.$$

Problème 5 : Le théorème fondamental de l'arithmétique pour $\mathbb{Z}[i]$
Démontrez le théorème fondamental de l'arithmétique : pour tout entier de Gauss $x \in \mathbb{Z}[i]$, il existe une *unique* factorisation de x en nombres premiers

$$x = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_n^{\alpha_n}.$$

Indication : on utilisera le fait que $\mathbb{Z}[i]$ est un anneau euclidien pour trouver une telle factorisation, puis le lemme de Gauss pour en démontrer l'unicité.

Problème 6 : Les premiers de Gauss
On veut étudier quels sont les nombres premiers dans $\mathbb{Z}[i]$.

1. Montrer que 2 n'est pas un nombre premier, mais qu'il correspond au carré d'un nombre premier à une unité près.
2. Montrer que tout nombre congru à 1 modulo 4 qui est premier dans $\mathbb{Z}$ ne l'est plus dans $\mathbb{Z}[i]$. *Indication : on utilisera les résultats de la feuille précédente.*

   On définit maintenant la fonction *norme* $N : \mathbb{Z}[i] \to \mathbb{Z}$ par la formule :

   $$N(a + bi) = a^2 + b^2.$$

3. Montrer que l'on a $N(x) = x \cdot \bar{x}$ pour tout $x \in \mathbb{Z}[i]$, où "$\bar{}$" représente la conjugaison complexe. Montrer par ailleurs que la norme est multiplicative, i.e. que l'on a
   $$N(x \cdot y) = N(x) \cdot N(y) \quad \forall\, x, y \in \mathbb{Z}[i].$$
4. Soit maintenant $q \in \mathbb{Z}[i]$ un premier de Gauss. Montrer que $N(q)$ divise p^2 pour un certain nombre entier p premier dans $\mathbb{Z}$. En déduire que soit $N(q)$ est premier dans $\mathbb{Z}$, soit il est le carré d'un nombre premier dans $\mathbb{Z}$.
5. Montrer que si $N(q) = p^2$, alors on a $q = pu$ et $\bar{q} = p\bar{u}$ avec u une unité dans $\mathbb{Z}[i]$. En déduire que p est dans ce cas congru à 3 modulo 4.
6. Montrer que, dans le sens inverse, tout entier premier dans $\mathbb{Z}$ et congru à 3 modulo 4 est un premier de Gauss. *Indication : on raisonnera par l'absurde et on utilisera la multiplicativité de la norme ainsi que les résultats de la feuille précédente.*
7. Montrer que si $N(q) = p$, alors on a $p = 2$ ou p congru à 1 modulo 4.
8. Conclure la classification des premiers de Gauss.