Echanges

En réponse à une question de J.DIEUDONNÉ

Une famille d'anneaux intègres non factoriels.

Guy Heuzé
Université de Toulouse Le Mirail

Il est traditionnel de présenter $\mathbf{Z}[i\sqrt{5}]$ comme contre-exemple.

Or, tout $\mathbf{Z}[i\sqrt{p}]$ convient avec p premier ≥ 3, ce que je n'ai lu nulle part. La vérification en est facile.

1-Dans un anneau intègre ,
- les *inversibles* sont les diviseurs de **1,**
- un élément a est *irréductible* s'il n'est pas inversible et si ses seuls diviseurs sont les inversibles et les éléments de la formule ua où u est inversible.

2-Un anneau est *factoriel* si :
- il est intègre,
- tout élément non nul et non inversible est produit d'un nombre fini d'irréductibles,

- quand un irréductible divise un produit, il divise au moins un des facteurs (condition équivalente à "l'unicité" de la factorisation obtenue en application de l'axiome précédent).

3-Etude de $A = \mathbb{Z}[i\sqrt{p}]$ avec p premier ≥ 3.

A est le sous anneau de C engendré par $i\sqrt{p}$,

donc $A = \{ a + i\sqrt{p}\, b \mid a, b \in \mathbb{Z} \}$

(on pourrait encore écrire $= \mathbb{Z} + i\sqrt{p}\,\mathbb{Z}$).

(3.1) ***A est intègre.***
Car c'est un sous anneau de C.

(3.2) $(a + i\sqrt{p}\, b)$ ***divise*** $(c + i\sqrt{p}\, d)$ ***si et seulement si le système*** $\begin{cases} ax - pby = c \\ bx + ay = d \end{cases}$ ***a une solution entière.***

C'est la traduction de $(a + i\sqrt{p}\, b)(x + i\sqrt{p}\, y) = c + i\sqrt{p}\, d$.

(3.3) ***Pour que*** $(a + i\sqrt{p}\, b)$ ***divise*** $(c + i\sqrt{p}\, d)$ ***il faut que*** $(a^2 + p\, b^2)$ ***divise*** $(c^2 + p\, d^2)$.
$z = a + i\sqrt{p}\, b$ étant un élément de A, posons $N(z) = z\,\bar{z} = a^2 + p\, b^2$. On a alors $N(z\, z') = N(z)\, N(z')$.

(3.4) ***Les inversibles de A sont 1 et - 1.***
Si z est inversibles, on a $z\, z' = 1$, d'où $N(z)\, N(z') = 1$.
Donc $N(z) = 1$ et $z = \pm 1$.
Remarquons que si z n'est pas inversible, alors $N(z) > 1$.

(3.5) ***Tout élément non nul et non inversible de A est produit d'un nombre fini d'irréductibles.***
La démonstration se fait par récurrence sur $N(z)$.
Si z n'est pas irréductible, on a $z = z'\, z''$ où z' et z'' ne sont pas inversibles.
Donc $N(z') > 1$ et $N(z'') > 1$.
D'où $N(z') < N(z)$ et $N(z'') < N(z)$;
z' et z'' vérifiant la proposition du fait de l'hypothèse de récurrence, z la vérifie donc aussi.

(3.6) **2** ***est irréductible de*** **A.**
Si $z\,z' = 2$, on a $N(z)\,N(z') = 4$.
Or, $N(z) = 2$ est impossible avec $p \geq 3$.

(3.7) **2** ***ne divise pas*** $(1 + i\sqrt{p})$ *(ni* $(1 - i\sqrt{p})$ *par conjugaison)*

Car $2\,(a + i\sqrt{p}\,b) = c + i\sqrt{p}\,d$ impose c pair.

Remarque : en fait, $(1 + i\sqrt{p})$ est irréductible (donc aussi $(1 - i\sqrt{p})$)

(3.8) **2** ***divise*** $(1 + i\sqrt{p})(1 - i\sqrt{p})$.

Car $(1 + i\sqrt{p})(1 - i\sqrt{p}) = 1 + p$ où p est impair.

(3.9) **A** ***n'est donc pas factoriel.***

4- Remarque. Dans «Pour l'honneur de l'esprit humain», J.DIEUDONNÉ

$$\mathbf{Z}[i\sqrt{3}]\ ,\ \mathbf{Z}[i\sqrt{7}]\ ,\ \mathbf{Z}[i\sqrt{11}]$$

signale (p.191) qu'on s'interroge pour savoir si les anneaux
peuvent être munis d'une structure d'anneaux «euclidiens». La réponse est négative, car sinon, ils seraient "principaux", donc factoriels.