Université Paris 7 - Denis Diderot — 2018-2019
UFR de Mathématiques — M1 - Arithmétique

Feuille d'exercices 7

Exercice 1 1. Montrer les égalités suivantes

$$\mathbb{Z}[i]^* = \{\pm 1, \pm i\},\ A_0^* = \{\pm 1, \pm i, \pm j, \pm k\} \text{ et } A^* = A_0^* \bigcup \left\{ \frac{\pm 1 \pm i \pm j \pm k}{2} \right\}.$$

2. Montrer que A_0 n'est pas principal (à gauche).
3. Montrer qu'un élément de norme égale à un premier est irréductible.

Exercice 2 1. Montrer que $1+i$ est irréductible dans $\mathbb{Z}[i]$ et que $2 = -i(1+i)^2$.

2. Montrer que si $p \equiv 1 \bmod 4$ est un nombre premier, alors $p = \pi\bar{\pi}$ où π et son conjugué complexe $\bar{\pi}$ sont des irréductibles non associés de $\mathbb{Z}[i]$.
3. Montrer que si $p \equiv 3 \bmod 4$ est un nombre premier, alors p est irréductible dans $\mathbb{Z}[i]$.
4. Montrer que si π est un irréductible de $\mathbb{Z}[i]$ alors $\pi\mathbb{Z}[i] \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$ engendré par un nombre premier. En déduire que si π est un irréductible de $\mathbb{Z}[i]$ alors π divise un et un seul nombre premier usuel.
5. En déduire un classification des irréductibles de $\mathbb{Z}[i]$.

Exercice 3 Montrer que si $p \equiv 1 \bmod 4$ est un nombre premier, il existe exactement 8 couples $(a, b) \in \mathbb{Z}^2$ tels que $a^2 + b^2 = p$.

Exercice 4 Factoriser $-3 + 15i$ dans $\mathbb{Z}[i]$.

Exercice 5 Si B est un anneau commutatif, on définit $\mathbb{H}_B$ comme le groupe additif

$$\mathbb{H}_B = \{x1 + yi + zj + tk \mid x, y, z, t \in B\}$$

muni de la multiplication B-linéaire de même table que celle de $\mathbb{H}$. Remarquons que $A_0 = \mathbb{H}_{\mathbb{Z}}$ et que $A \subset \mathbb{H}_{\mathbb{Z}[\frac{1}{2}]}$. (On pourrait voir aussi $\mathbb{H}_B$ comme le produit tensoriel $\mathbb{H}_B = A_0 \otimes_{\mathbb{Z}} B$.)

1. Soit F un corps de caractéristique $\neq 2$ contenant deux élément a et b tels que $a^2 + b^2 + 1 = 0$. Montrer que l'application de $\mathbb{H}_F$ vers l'algèbre des matrices 2×2 à coefficients dans F définie par

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ i \mapsto \begin{pmatrix} a & b \\ b & -a \end{pmatrix},\ j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ et } k \mapsto \begin{pmatrix} b & a \\ a & -b \end{pmatrix}.$$

est un isomorphisme de F-algèbres.

2. Si p est premier impair, conclure que $\mathbb{H}_{\mathbb{F}_p}$ est isomorphe à l'algèbre des matrices 2×2 à coefficients dans $\mathbb{F}_p$.

Exercice 6 On veut montrer que $A^* \cong \mathrm{SL}_2(\mathbb{F}_3)$.

1. L'homomorphisme de réduction modulo 3 de $\mathbb{Z}[\frac{1}{2}]$ vers $\mathbb{F}_3$ induit un homomorphisme d'anneaux de $\mathbb{H}_{\mathbb{Z}[\frac{1}{2}]}$ vers $\mathbb{H}_{\mathbb{F}_3}$. En déduire un homomorphisme de groupe $\varphi\colon A^* \to \mathbb{H}_{\mathbb{F}_3}^* \cong \mathrm{GL}_2(\mathbb{F}_3)$.
2. Soit $m \in A^*$ tel que $m^2 = 1$ (resp. $m^3 = 1$). Montrer que si $m \equiv 1 \bmod 3$, alors $m = 1$. En déduire que $\ker(\varphi) = \{1\}$.
3. Conclure que A^* est isomorphe à un sous-groupe d'indice deux de $\mathrm{GL}_2(\mathbb{F}_3)$, qui doit donc être égal à $\mathrm{SL}_2(\mathbb{F}_3)$.