Devoir maison n^o 1

Exercice 1 (Extrait du sujet d'examen session 2 de 2018)

1. Soit $A = Z/25\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/2018\mathbf{Z}$. Donner les facteurs invariants des groupes abéliens $(A, +)$ et $(A^\times, \cdot)$.
2. Donner une base adaptée pour le sous-$\mathbf{Z}$-module $M \subset \mathbf{Z}^4$ engendré par $(2, -1, 0, 0)$, $(-1, 2, -1, -1)$, $(0, -1, 2, 0)$ et $(0, -1, 0, 2)$. Calculer le quotient $\mathbf{Z}^4/M$.

Exercice 2 (Théorème des deux carrés)

On considère l'anneau $\mathbf{Z}[i]$ des entiers de Gauss. Si $a + bi \in \mathbf{Z}[i]$ on définit $N(a + bi) = a^2 + b^2 = (a + bi)(a - bi)$. Dans la première question on redémontre quelques propriétés bien connues de $\mathbf{Z}[i]$.

1. Démontrez les propriétés suivantes :
   (a) Pour tout $(x, y) \in \mathbf{Z}[i]^2$, $N(xy) = N(x)N(y)$
   (b) $\mathbf{Z}[i]^\times = \{\pm 1, \pm i\}$
   (c) Pour tout $(x, y) \in \mathbf{Z}[i]^2$, $y \neq 0$, il existe $(q, r) \in \mathbf{Z}[i]^2$ tels que $x = yq + r$ avec $N(r) < N(y)$ (l'anneau $\mathbf{Z}[i]$ est donc Euclidien).

Soit M un $\mathbf{Z}$-module de type fini tel qu'il existe un endomorphisme J de M vérifiant $J^2 = -1$.

2. Montrez qu'on peut munir M d'une structure de $\mathbf{Z}[i]$-module de type fini.

On suppose désormais que M est un $\mathbf{Z}$-module libre.

3. Montrez que M est libre en tant que $\mathbf{Z}[i]$-module.
4. Montrez que le rang de M sur $\mathbf{Z}$ est pair, disons égal à $2r$, et qu'il existe une base du $\mathbf{Z}$-module M dans laquelle la matrice de J est
$$\begin{pmatrix} 0 & -I_r \\ I_r & 0 \end{pmatrix}$$
5. Si $x = a + bi \in \mathbf{Z}[i]$, montrer que $\mathbf{Z}[i]/(x)$ est fini de cardinal $a^2 + b^2$.
6. Soit $S = \{a^2 + b^2 \mid (a, b) \in \mathbf{Z}^2\}$ et soit p un nombre premier impair. Montrez que p appartient à S si et seulement si p est congru à 1 modulo 4 (il pourra être utile de munir $\mathbf{Z}/p\mathbf{Z}$ d'une structure de $\mathbf{Z}[i]$-module).

Exercice 3 (Lemme de Schur)

Soit A un anneau commutatif et unitaire. Un A-module est dit *simple* s'il est non nul et s'il ne possède aucun sous-module propre non nul.

1. Montrez qu'un module simple est isomorphe à un quotient A/I où I est un idéal maximal de A.
2. Montrez qu'un morphisme $f : M_1 \to M_2$ entre deux A-modules simples et soit nul, soit un isomorphisme.
3. En déduire que l'anneau des endomorphismes d'un module simple est une algèbre à division (i.e. un corps non nécessairement commutatif).