Devoir maison n^o 1, corrigé succint

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 $(A^\times, \cdot)$.
   On applique le théorème des restes chinois et on se rappelle que, si p est premier, $(\mathbf{Z}/p^k\mathbf{Z})^\times$ est d'ordre $p^k - p^{k-1}$ et est de plus cyclique si $p \neq 2$. On obtient que les diviseurs élémentaires de $(A, +)$ sont $2, 2, 3, 25, 1009$ et ses facteurs invariants sont $2, 2 * 3 * 25 * 1009 = 151350$, et que les diviseurs élémentaires de $(A^\times, \times)$ sont $2, 4, 16, 9, 5, 7$ et ses facteurs invariants $2, 4, 16 * 9 * 5 * 7 = 5040$.
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 $\mathbf{Z}^4/M$.

Soit M la matrice dont les colonnes sont les 4 vecteurs. On réalise des changements de base en effectuant des opérations élémentaires sur les colonnes, en tentant de trianguler la matrice. Sur cet exemple cela suffit à mettre en évidence une base adaptée, et il n'est pas indispensable d'appliquer l'algorithme de réduction de Gauss vu en cours. Par exemple, la succession des transformations suivantes : $C_1 \leftrightarrow -C_2$, $C_2 \leftarrow C_2 - 2C_1$, $C_2 \leftrightarrow -C_3$, $C_3 \leftarrow C_3 - 3C_2$, $C_3 \leftarrow C_3 + C_2$, $-C_3 \leftrightarrow C_4$, $C_4 \leftarrow C_4 - 2C_3$ conduit à la matrice

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 1 & -2 & 2 & 0 \\ 1 & 0 & -2 & 2 \end{pmatrix}$$

On en déduit que $e_1 = (1, -2, 1, 1)$, $e_2 = (0, 1, -2, 0)$, $e_3 = (0, 0, 1, -1)$, $e_4 = (0, 0, 0, 1)$ est une base de $\mathbf{Z}^4$ (puisque son déterminant est 1) adaptée à M (puisque $\{e_1, e_2, 2e_3, 2e_4\}$ est une base de M), et que $\mathbf{Z}^4/M$ est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

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 $(x, y) \in \mathbf{Z}[i]^2$, $N(xy) = N(x)N(y)$
   C'est évident en remarquant que $N(x) = x\overline{x}$
   (b) $\mathbf{Z}[i]^\times = \{\pm 1, \pm i\}$
   Soit $x \in \mathbf{Z}[i]^\times$. Si $xy = 1$ alors $N(x)N(y) = 1$ ce qui montre que $N(x) \in \mathbf{Z}^\times = \{\pm 1\}$. On en déduit aisément le résultat.
   (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).
   On considère $xy^{-1} \in \mathbf{Q}[i]$. On écrit $xy^{-1} = a + bi$ avec $a, b \in \mathbf{Q}$ et on pose $q = a_0 + b_0 i$ où a_0 et b_0 sont les entiers les plus proches de respectivement a et b. Alors $|a - a_0| \leq 1/2$ et $|b - b_0| \leq 1/2$ donc, si $u = xy^{-1} - q$ on a $N(u) \leq 1/4 + 1/4 < 1$ d'où le résultat avec $r = uy$.

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.
   Comme $J^2 = -\mathrm{Id}$, on a un morphisme f de $\mathbf{Z}[i]$ dans $\mathrm{End}(M)$ en posant $f(a + bi) = a + bJ$. D'après le cours, cela revient à munir M d'une structure de $\mathbf{Z}[i]$-module. S'il est de type fini sur $\mathbf{Z}$ alors il est à fortiori de type fini sur $\mathbf{Z}[i]$ car une famille $\mathbf{Z}$-génératrice de M est aussi $\mathbf{Z}[i]$-génératrice.

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

3. Montrez que M est libre en tant que $\mathbf{Z}[i]$-module.

   Comme $\mathbf{Z}[i]$ est principal (on a vu qu'il est Euclidien), il suffit de montrer qu'il est sans torsion. Supposons $m \in M$, $m \neq 0$ et $x \in \mathbf{Z}[i]$ tels que $xm = 0$. Alors on multiplie par $\overline{x}$ pour obtenir $N(x)m = 0$. Mais $N(x) \in \mathbf{Z}$ et M est sans $\mathbf{Z}$-torsion (car $\mathbf{Z}$-libre) donc on en déduit que $N(x) = 0$ et donc que $x = 0$.

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

$$\begin{pmatrix} 0 & -I_r \\ I_r & 0 \end{pmatrix}$$

   On vérifie que si $\{e_1, \ldots, e_k\}$ est une $\mathbf{Z}[i]$-base de M, alors $\{e_1, \ldots, e_k, ie_1, \ldots, ie_k\}$ est une $\mathbf{Z}$-base de M qui est donc de $\mathbf{Z}$-rang pair. De plus, comme $J(e_j) = ie_j$ et $J(ie_j) = J^2(e_j) = -e_j$, la matrice de J dans cette base est bien comme annoncée.

5. Si $x = a + bi \in \mathbf{Z}[i]$, montrer que $\mathbf{Z}[i]/(x)$ est fini de cardinal $a^2 + b^2$.

   On va appliquer le résultat de l'exercice 6 de la feuille 2. On voit $(x) = x\mathbf{Z}[i]$ comme l'image de l'endomorphisme de $\mathbf{Z}$-modules $f : \mathbf{Z}[i] \to \mathbf{Z}[i]$ défini par : $f(y) = xy$ qui est clairement injectif. Dans la $\mathbf{Z}$-base $\{1, i\}$ sa matrice est $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ et est de déterminant $a^2 + b^2$. Donc le cardinal du quotient $\mathbf{Z}[i]/(x)$ est bien $a^2 + b^2$.

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).

   Supposons d'abord que $p \in S$. Le carré d'un nombre entier est toujours congru à 0 ou 1 modulo 4 donc un nombre de la forme $a^2 + b^2$ est congru à $0, 1$ ou 2 modulo 4. Comme p est supposé impair, il ne peut être congru à 0 ou à 2 d'où le résultat. Réciproquement, supposons $p \equiv 1 \bmod 4$. Alors $(-1)^{(p-1)/2} = 1$ ce qui montre que -1 est un carré modulo p. Si $-1 = J^2$ avec $J \in \mathbf{Z}/p\mathbf{Z}$, la multiplication par J est un endomorphisme de $\mathbf{Z}/p\mathbf{Z}$ vu comme $\mathbf{Z}$-module. D'après la question 2., on peut munir $\mathbf{Z}/p\mathbf{Z}$ d'une structure de $\mathbf{Z}[i]$-module. Il est évidemment de type fini et de torsion. Par le théorème de structure, il existe $x_1, \ldots, x_k$ tels que $\mathbf{Z}/p\mathbf{Z} \simeq \prod_{j=1}^{k} \mathbf{Z}[i]/(x_j)$ et on en déduit en considérant les cardinaux et grâce à la question 5. que $p = \prod N(x_j)$. Enfin, comme $\prod N(x_j) = N(\prod x_j)$, on a $p \in S$.

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.

   Soit M un A-module simple et soit $x \in M$ tel que $Ax \neq \{0\}$. Comme Ax est un sous-module de M, on a $Ax = M$. On a donc un morphisme surjectif de A sur M défini par $f(a) = ax$. Son noyau est un idéal I de A et $A/I \simeq M$ par le théorème de factorisation. Si I n'était pas maximal on aurait $I \subset J \subset A$ avec des inclusions strictes et J/I serait isomorphe par f à un sous-module strict de M.

2. Montrez qu'un morphisme $f : M_1 \to M_2$ entre deux A-modules simples et soit nul, soit un isomorphisme.

   $\operatorname{Ker} f$ *et* $\operatorname{Im} f$ *sont des sous-modules de respectivement M_1 et M_2 qui sont simples donc les seules possibilités sont* $\operatorname{Ker} f = \{0\}$ *ou M_1 et* $\operatorname{Im} f = \{0\}$ *ou M_2.*

3. En déduire que l'anneau des endomorphismes d'un module simple est une algèbre à division (i.e. un corps non nécessairement commutatif).

   On a vu à la question précédente qu'un endomorphisme non nul d'un module simple est nécessairement un isomorphisme.