Devoir surveillé, corrigé succint

Exercice 1 : Voir le cours !

Exercice 2 : On a $\mathrm{pgcd}(35,10) = 5$. Les nombres $(7,2)$ sont premiers entre eux et forment la première ligne de la matrice de $\mathbf{GL}_2(\mathbf{Z})$: $\begin{pmatrix} 7 & 2 \\ 3 & 1 \end{pmatrix}$ (donnée par la relation de Bezout $7*1-2*3=1$). On peut donc écrire

$$\begin{pmatrix} 14 & 35 & 10 \end{pmatrix} = \begin{pmatrix} 14 & 5 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 7 & 2 \\ 0 & 3 & 1 \end{pmatrix}$$

où la matrice est dans $\mathbf{GL}_3(\mathbf{Z})$. Les nombre 14 et 5 sont premiers entre eux avec $14*1-5*3=-1$ ce qui conduit à :

$$\begin{pmatrix} 14 & 5 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 14 & 5 & 0 \\ 3 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

et, à nouveau, la matrice est dans $\mathbf{GL}_3(\mathbf{Z})$. Finalement on obtient en combinant les deux expressions :

$$\begin{pmatrix} 14 & 35 & 10 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 14 & 5 & 0 \\ 3 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 7 & 2 \\ 0 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 14 & 35 & 10 \\ 3 & 7 & 2 \\ 0 & 3 & 1 \end{pmatrix}$$

et on a obtenu une matrice de $\mathbf{GL}_3(\mathbf{Z})$ dont la première ligne est $(14, 35, 10)$.

Exercice 3 :

1. M est fini donc il est à fortiori de type fini, engendré par lui-même.
2. On décompose les nombres en produits de facteurs premiers : $350 = 2 \cdot 5^2 \cdot 7$, $144 = 2^4 \cdot 3^2$, $216 = 2^3 \cdot 3^3$, $49 = 7^2$. D'après le théorème des restes chinois :

   $$M \simeq (\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/5^2\mathbf{Z} \times \mathbf{Z}/7\mathbf{Z}) \times (\mathbf{Z}/2^4\mathbf{Z} \times \mathbf{Z}/3^2\mathbf{Z}) \times (\mathbf{Z}/2^3\mathbf{Z} \times Z/3^3\mathbf{Z}) \times (\mathbf{Z}/7^2\mathbf{Z}).$$

   Les diviseurs élémentaires de M sont donc : $2, 2^3, 2^4, 3^2, 3^3, 5^2, 7, 7^2$.
3. Pour obtenir les facteurs invariants on regroupe les diviseurs élémentaires suivant le tableau suivant :

premiers			
2	2	2^3	2^4
3	1	3^2	3^3
5	1	1	5^2
7	1	7	7^2
produit	2	504	529200

   Par le théorème chinois, on obtient

   $$M \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/504\mathbf{Z} \times \mathbf{Z}/529200\mathbf{Z}$$

   et par construction $2 \mid 504 \mid 529200$ donc les facteurs invariants de M sont $2, 504, 529200$.
4. $\mathrm{Ann}(M) = 529200\mathbf{Z}$.
5. les composantes p-primaires de M sont :
   $M_2 = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^3\mathbf{Z} \times \mathbf{Z}/2^4\mathbf{Z}$
   $M_3 = \mathbf{Z}/3^2\mathbf{Z} \times \mathbf{Z}/3^3\mathbf{Z}$
   $M_5 = \mathbf{Z}/5^2\mathbf{Z}$
   $M_7 = \mathbf{Z}/7\mathbf{Z} \times \mathbf{Z}/7^2\mathbf{Z}$
   $M_p = \{0\}$ pour tout $p \neq 2, 3, 5, 7$.

6. Il est clair que $M(p)$ est un $\mathbf{Z}$-sous-module de M car il est stable par addition et par multiplication par les éléments de $\mathbf{Z}$. De plus, par définition il est annulé par p : pour tout $v \in M(p)$, on a $p \cdot v = 0$. Donc si $\overline{k} \in \mathbf{Z}/p\mathbf{Z}$, on peut définir sans ambiguité $\overline{k} \cdot v$ par : $\overline{k} \cdot v = k \cdot v$ (en effet si $\overline{k} = \overline{\ell}$ alors $k \cdot v = \ell \cdot v$), ce qui munit $M(p)$ d'une structure de $\mathbf{Z}/p\mathbf{Z}$-module. Comme $\mathbf{Z}/p\mathbf{Z}$ est un corps si p est premier, c'est donc bien un $\mathbf{Z}/p\mathbf{Z}$-espace vectoriel.
7. Il est clair que $M(2) \subset M_2$ et que $M(2) = \mathbf{Z}/2\mathbf{Z} \times 2^2\mathbf{Z}/2^3\mathbf{Z} \times 2^3\mathbf{Z}/2^4\mathbf{Z} \simeq (\mathbf{Z}/2\mathbf{Z})^3$. Donc $\dim M(2) = 3$.
8. $\dim M(3) = 2$, $\dim M(5) = 1$, $\dim M(7) = 2$ et $\dim M(11) = 0$.

Exercice 4 : Par le théorème de structure des $\mathbf{Z}$-modules de type fini, Il y a autant de classes d'isomorphisme de groupes commutatifs d'ordre 72 que d'entiers positifs $(a_1, \dots, a_k)$ tels que $a_1 \mid \cdots \mid a_k$ avec $a_1 \dots a_k = 72$. Comme $72 = 2^3 \cdot 3^2$, on a les possibilités suivantes : $(2^3 \cdot 3^2)$; $(2, 2^2 \cdot 3^2)$; $(2, 2, 2 \cdot 3^2)$; $(3, 2^3 \cdot 3)$; $(2 \cdot 3, 2^2 \cdot 3)$; $(2, 2 \cdot 3, 2 \cdot 3)$ ce qui conduit aux 6 classes s'isomorphisme de groupes :

$$\begin{array}{ccc} \mathbf{Z}/72\mathbf{Z} & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/36\mathbf{Z} & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/18\mathbf{Z} \\ \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/24\mathbf{Z} & \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z} & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z} \end{array}$$

Exercice 5 :

1. Les opérations sur $\mathrm{End}_A(M)$ sont définies à partir de celles de M : l'addition de deux éléments $(f, g) \in \mathrm{End}_A(M)^2$ est définie par $(f+g)(x) = f(x) + g(x)$ pour tout $x \in M$, et la multiplication par $a \in A$ est définie par : $(a \cdot f)(x) = a \cdot f(x)$. Il faut ensuite vérifier que $f + g \in \mathrm{End}_A(M)$, que $a \cdot f \in \mathrm{End}_A(M)$, et que ces opérations satisfont aux propriétés de module, ce qui est fastidieux mais élémentaire.
2. La suite des sous-modules $\mathrm{Ker}(u^n)$ est croissante pour l'inclusion. Puisque M est noethérien, elle est stationnaire, c'est-à-dire il existe un entier n_0 tel que $\mathrm{Ker}(u^n) = \mathrm{Ker}(u^{n_0})$ pour tout $n \geq n_0$. Soit maintenant $u \in \mathrm{End}_A(M)$ surjectif, et soit $x \in \mathrm{Ker}(u)$. Puisque u est surjectif, u^{n_0} l'est aussi et on peut écrire $x = u^{n_0}(y)$ pour un $y \in M$. Alors $u(x) = u^{n_0+1}(y) = 0$ donc $y \in \mathrm{Ker}(u^{n_0+1})$. Comme $\mathrm{Ker}(u^{n_0+1}) = \mathrm{Ker}(u^{n_0})$, on en déduit que $y \in \mathrm{Ker}(u^{n_0})$, soit $u^{n_0}(y) = 0$ i.e. $x = 0$. On a donc montré que $\mathrm{Ker}(u) = \{0\}$ donc que u est injectif.
3. On peut prendre $M = A = \mathbf{Z}$ et $u : \mathbf{Z} \to \mathbf{Z}$ défini par $u(x) = 2x$. L'image de u est $2\mathbf{Z} \neq \mathbf{Z}$ donc u n'est pas surjectif ; u est clairement injectif.
4. On note $A^{(\mathbf{N})}$ l'ensemble des suites à valeurs dans A et à support fini. C'est un A-module. Pour montrer que M n'est pas noethérien, on construit une suite croissante de sous-modules qui n'est pas stationnaire : soit $M_k = \{a = (a_n)_{n \geq 0} \in M \mid a_n = 0 \text{ pour tout } n \geq k\}$. On a clairement $M_k \subset M_{k+1}$ et $M_k \neq M_{k+1}$.
5. On a $a_0, a_1, \cdots = u(0, a_0, a_1, \dots)$ donc u est surjective et $\mathrm{Ker}(u) = \{a_0, 0, 0, \cdots \mid a_0 \in A\}$ donc u n'est pas injective.
6. Soit $x = p/q \in \mathbf{Q}$ et soit $\overline{x}$ sa classe modulo $\mathbf{Z}$. Alors $\overline{x} = u(\overline{x/2})$ donc u est bien surjective. Par ailleurs, $u(\overline{1/2}) = \overline{1} = 0$ donc $\overline{1/2} \in \mathrm{Ker}(u)$ et est non nul, donc u n'est pas injective. D'après la question 2., l'existence de u montre que M n'est pas noethérien. Comme $\mathbf{Z}$ est un anneau noethérien, si M était de type fini il serait noethérien par un théorème du cours, donc il n'est pas de type fini.

Exercice 6 :

1. A est principal car il est euclidien comme tout anneau de polynômes à coefficients dans un corps.
2. Montrons que $A^\times = \mathbf{R}^\times$: en effet, si $P(x)Q(x) = 1$ en comparant les degrés on a $\deg(P) + \deg(Q) = 0$ soit $\deg(P) = \deg(Q) = 0$ soit P et Q sont des polynômes constants non nuls.
3. Soit $P(x)$ un polynôme de degré 1. Si $P = Q_1Q_2$ alors $1 = \deg(Q_1) + \deg(Q_2)$ ce qui impose que $\deg(Q_1)$ ou $\deg(Q_2)$ soit nul, c'est-à-dire que Q_1 ou Q_2 soit un inversible. Donc P est irréductible.
4. Un polynôme de degré 2 ne peut avoir pour diviseurs stricts que des polynômes de degré 1. Il est donc irréductible dans A si et seulement s'il n'a pas de racines dans $\mathbf{R}$ ce qui équivaut à la condition $\Delta < 0$ où Δ est son discriminant.
5. Les irréductibles de A sont à association près les polynômes unitaires de degré 1 et les polynômes unitaires de degré 2 et de discriminant négatif. En effet, un polynôme $P(x) \in A$ de degré $d \geq 3$ possède au moins une racine complexe z (car $\mathbf{C}$ est algébriquement clos). Si $z \in \mathbf{R}$, $P(x)$ est divisible dans A par $x - z$. Si $z \notin \mathbf{R}$, alors $\overline{z}$ est aussi racine de P, $Q := (x-z)(x-\overline{z}) \in \mathbf{R}[x]$ et divise P. Dans tous les cas P n'est pas un irréductible de A.
6. On a les factorisations suivantes :
   $a_1(x) = x^3(x+1)$
   $a_2(x) = x(x-1)^2(x+1)^2$
   $a_3(x) = x^4(x^2+x+1)$
   $a_4(x) = (x-1)^2(x^2+x+1)^2$
7. Les diviseurs élémentaires sont :
   $x, x^3, x^4, (x+1), (x+1)^2, (x-1)^2, (x-1)^2, (x^2+x+1), (x^2+x+1)^2$.
   Les facteurs invariants sont :
   $x, x^3(x+1)(x-1)^2(x^2+x+1), x^4(x+1)^2(x-1)^2(x^2+x+1)^2$.
   Les composantes p-primaires non nulles de M sont :
   $M_x = (A/xA) \oplus (A/x^2A) \oplus (A/x^4A)$.
   $M_{(x+1)} = A/(x+1)A \oplus A/(x+1)^2A$.
   $M_{(x-1)} = A/(x-1)^2A \oplus A/(x-1)^2A$.
   $M_{(x^2+x+1)} = A/(x^2+x+1)A \oplus A/(x^2+x+1)^2A$.
8. Même argument que pour la question 6. de l'exercice 3 : $M(P(x))$ est un $\mathbf{R}[x]$-module car c'est un sous-module de M ; il est (par définition) annulé par $P(x)$ donc c'est un $\mathbf{R}[x]/P(x)\mathbf{R}[x]$-module. Comme $P(x)$ est irréductible, le quotient $\mathbf{R}[x]/P(x)\mathbf{R}[x]$ est un corps.
9. On a $\mathbf{R}[x]/x\mathbf{R}[x] \simeq \mathbf{R}$. En effet si $Q(x) = \sum_{i=0}^{k} a_i x^i \in \mathbf{R}[x]$ alors $Q(x) \equiv a_0 \bmod x$. L'application $Q \mapsto a_0$ induit un isomorphisme entre $\mathbf{R}[x]/x\mathbf{R}[x]$ et $\mathbf{R}$. On a vu que $M_x = (A/xA) \oplus (A/x^2A) \oplus (A/x^4A)$ donc
   $$M(x) = (A/xA) \oplus (xA/x^2A) \oplus (x^3A/x^4A) \simeq (\mathbf{R}[x]/x\mathbf{R}[x])^3 \simeq \mathbf{R}^3$$
   donc $\dim_{\mathbf{R}} M(x) = 3$.
10. De même $\dim M(x^2+x+1) = 2$. Noter que $\mathbf{R}[x]/(x^2+x+1)\mathbf{R}[x] \simeq \mathbf{C}$.
