Feuille 3

Modules – Modules de type fini sur des anneaux principaux

1. Déterminer les ordres, les exposants, les facteurs invariants et les isomorphismes mutuels des groupes suivants : $\mathbf{Z}/72\mathbf{Z}$, $\mathbf{Z}/8\mathbf{Z}\times\mathbf{Z}/9\mathbf{Z}$, $\mathbf{Z}/54\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/9\mathbf{Z}$, $\mathbf{Z}/6\mathbf{Z}\times\mathbf{Z}/12\mathbf{Z}$, $\mathbf{Z}/18\mathbf{Z}\times\mathbf{Z}/4\mathbf{Z}$, $\mathbf{Z}/36\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/8\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/6\mathbf{Z}\times\mathbf{Z}/6\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$?

2. Montrer qu'un groupe abélien fini est cyclique si et seulement si il contient un sous-groupe isomorphe à $(\mathbf{Z}/p\mathbf{Z})^2$ avec p premier.

3. Considérons $\mathbf{R}$ muni de l'addition, $\mathbf{R}^*$ et $\mathbf{C}^*$ munis de la multiplication, comme des $\mathbf{Z}$-modules.
3.a. Soit n un entier ≥ 1. Soient p_1, p_2... p_n des nombres premiers. Montrer que la famille $(\log(p_i))_{i\in\{1,2...n\}}$ est libre dans le $\mathbf{Z}$-module $\mathbf{R}$, puis que $\mathbf{R}$ contient des $\mathbf{Z}$-modules libres de rangs arbitrairement grands.
3.b. Montrer que les groupes $\mathbf{R}^*$ et $\mathbf{C}^*$ contiennent des $\mathbf{Z}$-modules libres de rangs arbitrairement grands.
3.c. Les sous-groupes de type fini de $\mathbf{R}$, $\mathbf{R}^*$ et $\mathbf{C}^*$ sont-ils tous libres ?
3.d. Montrer qu'il existe un groupe abélien fini non isomorphe à un sous-groupe de $\mathbf{C}^*$.

4. Soit G un groupe abélien fini. On rappelle que l'*exposant* de G est le ppcm des ordres de ses éléments.
4.a. Soient x, $y \in G$ d'ordres respectivement n et m, premiers entre eux. Quel est l'ordre de $x + y$?
4.b. Montrer qu'il existe dans G un élément d'ordre égal à l'exposant de G.

5.a Soit A un anneau intègre et noethérien. Montrer que A est principal si et seulement si tous les A-modules de type fini sans torsion sont libres.
5.b. Soit A un anneau principal. Soient a, $b \in A$. Quels sont les facteurs invariants de $A/(a) \times A/(b)$?

6. Soit A un anneau commutatif. Soit M un A-module. On dit que M est *artinien* si toute suite décroissante de sous-modules de M est stationnaire et que A est un *anneau artinien* s'il est artinien en tant que A-module.
6.a. Montrer que M est artinien si et seulement si tout ensemble non-vide de sous-modules de M admet un élément minimal pour l'inclusion.
6.b. Montrer que $\mathbf{Z}$ et $K[X]$ ne sont pas des anneaux artiniens. Donner des exemples d'anneaux artiniens.
6.c. Montrer que tout groupe abélien fini est artinien.
6.d. Soit $f : M \to N$ A-linéaire. Montrer que si M est artinien, $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ le sont aussi.
6.e. Supposons l'anneau A artinien. Monter que tout A-module de type fini est artinien.
6.f. Supposons M artinien. Soit $f \in \mathrm{End}_A(M)$. Montrer que si f est injectif, f est bijectif.
6.g. Supposons M noethérien et artinien. Soit f une application A-linéaire $E \to E$. Montrer que la suite $\mathrm{Ker}(f^n)$ est croissante et que la suite $\mathrm{Im}(f^n)$ est décroissante.
6.h. Reprenons la question précédente. Montrer qu'il existe des sous-module I et N de M tels que $M = I \oplus N$ et que les restrictions de $f_{|I}$ soit un isomorphisme de A-modules et $f_{|I}$ soit un endomorphisme nilpotent.
6.i. Supposons que $A = K[X]$, avec K corps. Montrer que tout A-module de type fini et de torsion est artinien. En déduire qu'un K-espace vectoriel de dimension finie muni de la structure de $K[X]$-module donnée par un endomorphisme est un $K[X]$-module artinien.

7. Soit K un corps. Soit $A = K[X, Y]$. Soit I l'idéal de A engendré par $\{X, Y\}$. L'anneau A est-il principal ? Est-il factoriel ? Montrer que I est de type fini et sans torsion, mais n'est pas un A-module libre. Le théorème de structure des modules de type fini sur les anneaux principaux est-il encore valable pour les modules de type fini sur les anneaux factoriels ?

8. Soit M un $\mathbf{Z}$-module libre de base (e_1, e_2, e_3). Notons U le sous-module engendré par $\{3e_1 - 12e_2 + 10e_3, -12e_1 + 64e_2 - 60e_3, 10e_1 - 60e_2 + 60e_3\}$.
8.a. Trouver les invariants de U.
8.b. Montrer que M/U est isomorphe à $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/20\mathbf{Z}$.

9. Soit M un $\mathbf{Z}$-module libre de rang fini. Soit $f : M \to M$ un endomorphisme. Montrer que le conoyau de f est fini si et seulement si $\det(f) \neq 0$. Montrer que, dans ce cas, le conoyau de f a pour ordre $|\det(f)|$.

10. Soit n un entier ≥ 1. Notons $n = \prod_p p^{e_p}$ sa décomposition en produit de facteurs premiers.
10.a. Montrer que le groupe $(\mathbf{Z}/n\mathbf{Z})^*$ est isomorphe au produit $\prod_p (\mathbf{Z}/p^{e_p}\mathbf{Z})^*$.
10.b. Fixons désormais un nombre premier p. Soit $e \geq 1$. Quel est l'ordre de $(\mathbf{Z}/p^e\mathbf{Z})^*$?
10.c. Montrer que le noyau N_p de la réduction modulo p : $(\mathbf{Z}/p^e\mathbf{Z})^* \to (\mathbf{Z}/p\mathbf{Z})^*$ est un groupe d'ordre p^{e-1}.
10.d. Supposons que $p \neq 2$. Montrer par récurrence sur e que $(1+p)^{p^{e-1}} \equiv 1 + p^e \pmod{p^{e+1}}$.
10.e. Supposons que $p \neq 2$. En déduire que la classe de $1+p$ engendre N_p.
10.f. Supposons que $p \neq 2$. En déduire que $(\mathbf{Z}/p^e\mathbf{Z})^*$ est isomorphe au produit d'un groupe cyclique d'ordre p^{e-1} et d'un groupe cyclique d'ordre $p-1$. Est-il cyclique ? Comment en trouver un générateur ?
10.g. Si on a $e \geq 2$, montrer que le noyau de la réduction modulo 4 : $(\mathbf{Z}/2^e\mathbf{Z})^* \to (\mathbf{Z}/4\mathbf{Z})^*$ est d'ordre 2^{e-2}.
10.h. Montrer par récurrence sur e que $(5)^{2^{e-2}} \equiv 1 + 2^e \pmod{2^{e+1}}$.
10.i. En déduire que $(\mathbf{Z}/2^e\mathbf{Z})^*$ est isomorphe au produit d'un groupe cyclique d'ordre 2^{e-2} et d'un groupe cyclique d'ordre 2. Est-il cyclique ? Par quelle méthode peut-on en trouver un système de générateurs ?
10.j. Déterminer les entiers $n \geq 1$ pour lesquels $(\mathbf{Z}/n\mathbf{Z})^*$ est cyclique, est d'ordre pair, est un p-groupe.
10.k. Donner deux entiers n et m distincts et > 2017 tels que $(\mathbf{Z}/n\mathbf{Z})^*$ et $(\mathbf{Z}/m\mathbf{Z})^*$ sont isomorphes.
10.l. Soit G un groupe abélien fini. À quelle condition $(\mathbf{Z}/n\mathbf{Z})^*$ possède-t-il un sous-groupe isomorphe à G ?

11.a. Pour $(\mathbf{Z}/128\mathbf{Z})^*$, $(\mathbf{Z}/192\mathbf{Z})^*$ et $(\mathbf{Z}/85\mathbf{Z})^*$, déterminer : ordres, exposants et facteurs invariants.
11.b. Lesquels de ces groupes sont isomorphes entre eux ? Indiquer des systèmes de générateurs.

12.a. Indiquer les ordres, les exposants et les facteurs invariants des groupes $(\mathbf{Z}/2016\mathbf{Z})^*$ et $(\mathbf{Z}/2017\mathbf{Z})^*$.
12.b. Pour lequel est-il le plus aisé de trouver un système minimal de générateurs ?

13. Soient K un corps et $P \in K[X]$. Soit V un K-espace vectoriel de dimension finie muni d'un endomorphisme linéaire u de polynôme minimal égal à P. Supposons P irréductible. Montrer que la dimension de V est divisible par le degré de P. Est-ce encore vrai si P n'est pas irréductible ?

14. Soit K un corps. Soit E un K-espace vectoriel de dimension finie. Soit u un endomorphisme de E. Notons $L(u) = \{v \in \mathrm{End}(E)/u \circ v = v \circ u\}$ (c'est le *commutant* de u). On rappelle que u est dit *cyclique* s'il existe $x \in E$ et un entier $n \geq 1$ tel que la famille $(u^k(x))_{k \in \{0,1...n-1\}}$ est une base de E.
14.a. Montrer que $K[u] \subset L(u)$.
14.b. Monter qu'il existe P_1, P_2,..., $P_r \in K[X]$, avec $P_1|P_2$, $...P_{r-1}|P_r$ tels que E soit isomorphe comme $K[u]$ module à $\prod_{i=1}^r K[X]/(P_i)$. En déduire une décomposition en somme directe de $E = \oplus_i^r E_i$, avec E_i isomorphe à $K[X]/(P_i)$ en tant que $K[X]$-module. En déduire que pour tout i, le $K[X]$-module E_i est cyclique. Soit $x_i \in E_i$ tel que $(u^k(x_i))_{0 \leq k \leq d_i - 1}$, où d_i est le degré de P_i.
14.c. Montrer que l'anneau $K[u]$ est isomorphe à $K[X]/(P)$, où P est le polynôme minimal de u.
14.d. Montrer que $L(u)$ est un K-espace vectoriel isomorphe à $\prod_{i=1}^r \mathrm{Ker}(P_i(u))$ par $\phi : v \mapsto (v(x_i))_{1 \leq i \leq r}$.
14.e. Montrer que pour tout i le projecteur sur E_i parallèlement à $\oplus_{j \neq i} E_j$ est dans $L(u)$.
14.f. Soit $w \in L(L(u))$. Montrer qu'il existe $R \in K[X]$ tel que $w(x_r)) = R(u)x_r$.
14.g. Soit $v \in L(u)$ image réciproque de $(x_1, x_2...x_{r-1}, x_i)$ par ϕ. Montrer que $w(x_i) = R(u)x_i$.
14.h. Posons $L(L(u)) = \cap_{v \in L(u)} L(v)$. C'est le *bicommutant* de u. Montrer que $L(L(u)) = K[u]$.
14.i. Supposons le corps K infini. Montrer que les quatre propriétés suivantes sont équivalentes. *(i)* u est cyclique *(ii)* Le polynôme minimal de u coïncide avec son polynôme caractéristique *(iii)* On a l'égalité $L(u) = K[u]$ *(iv)* L'espace vectoriel E n'a qu'un nombre fini de sous-espaces vectoriels stables par u.

15. Soit K un corps. Soit $P \in K[X]$. Notons n son degré. On s'intéresse au nombre $s(P)$ de classes de similitudes de matrices de $M_n(K)$ ayant P pour polynôme caractéristique.
15.a. Déterminer $s(P)$ pour P est irréductible, puis pour $P = Q^e$, avec Q irréductible et e entier ≥ 1.
15.b. Déterminer $s(P)$ en général, à partir de la décomposition de P en produit de polynômes irréductibles.

16. Soit K un corps. On a vu que le sous-anneau $A = K[X^2, X^3]$ de $K[X]$ n'est pas principal, car l'idéal $I = (X^2, X^3)$ n'est pas principal. Considérons $f : A^2 \to I$ qui à (P, Q) associe $PX^2 + QX^3$. Notons N son noyau, d'où la suite exacte courte $0 \to N \to A^2 \to I \to 0$. On rappelle que $A \otimes_A I \simeq I$.
16.a. Montrer que I est sans torsion. Le module N est-il libre de rang 1 ?
16.b. Considérons l'application linéaire $f \otimes 1 : (A \otimes_A I)^2 \simeq I^2 \to I \otimes_A I$. Montrer qu'elle est surjective et que son noyau contient $N \otimes_A I$. Montrer que son noyau n'est pas $N \otimes_A I$. Autrement dit la suite $N \otimes_A I \to I^2 \to I \otimes_A I \to 0$ ne donne pas lieu à une suite exacte courte (*i.e.* le A-module I n'est pas plat).