Université Paris Diderot — Algèbre – Année 2019-20
M1 mathématiques

Feuille 5

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 ne contient pas 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 facteurs 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 et N deux groupes abéliens finis tels que $M\times M$ est isomorphe à $N\times N$. Montrer que M est isomorphe à N. Est-ce encore vrai si on remplace l'hypothèse "finis" par "de types finis".

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 > 2019 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. Soit K un corps. Soit V un K-espace vectoriel de dimension finie muni d'un endomorphisme linéaire u. Montrer que la loi $K[X] \times V \to V$ qui à (P, v) associe $P.v = P(u)(v)$ fait de V un $K[X]$-module. Montrer que ce $K[X]$-module est de type fini, puis que son rang est nul. Notons $d_1, ..., d_s$ ses diviseurs élémentaires. Donner le polynôme minimal et le polynôme caractéristique de u en fonction des diviseurs élémentaires.

14. 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 ?

15. Soit K un corps. Soit E un K-espace vectoriel. Soit u un endomorphisme K-linéaire de E. Cela fait de E un $K[X]$-module par l'application $K[X] \times E \to E$ qui à $(P, v) \mapsto P.v = P(u)(v)$.
15.a.Soit $P \in K[X]$ unitaire. Posons $P = a_0 + a_1 X + ... + a_{n-1}X^{n-1} + X^n$. Considérons l'endomorphisme K-linéaire de $K[X]/P$ donnée par la multiplication par X. Écrire sa matrice dans la base $(1, X, ..., X^{n-1})$ de $K[X]/P$. C'est la *matrice compagnon* de P. On la note C_P. Montrer que P est le polynôme caractéristique et le polynôme minimal de C_P.
15.b. Montrer qu'il existe s entier ≥ 0 et P_1, P_2, ..., $P_s \in K[X]$ tels que $P_i | P_{i+1}$ pour tout i tels que E est isomorphe comme $K[X]$-module à $\oplus_{i=1}^s K[X]/P_i$. Ces polynômes sont les *invariants de similitude* de u.
15.c. En déduire qu'il existe des sous-espaces vectoriels F_1,...,F_s stables par u tels que $E = F_1 \oplus ... \oplus F_s$ et tels que, pour tout i, F_i admette une base B_i dans laquelle la matrice de $u_{|F_i}$ soit C_{P_i}. Écrire la matrice de u dans la base $\oplus_{i=1}^n B_i$. (On l'appelle parfois *forme normale canonique* de u.)

16. 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.
16.a. Déterminer $s(P)$ pour P est irréductible, puis pour $P = Q^e$, avec Q irréductible et e entier ≥ 1.
16.b. Déterminer $s(P)$ en général, à partir de la décomposition de P en produit de polynômes irréductibles.

17. Soient m et n des entiers ≥ 0. Soit A un anneau principal. On dit que deux matrices B, C de $M_{m,n}(A)$ sont *équivalentes* si il existe $U \in \mathrm{GL}_n(A)$, $V \in \mathrm{GL}_m(A)$ telles que $C = UBV$.
17.a. Montrer que B et C sont équivalentes si et seulement si il existe des bases X et Y de A^n et A^m respectivement telles que C soit la matrice dans ces bases de l'application linéraire $u : A^n \to A^m$ associée à B.
17.b. Montrer qu'il existe une base $(e_1, ..., e_m)$ de A^m et une suite finie et multiplicativement croissante $(d_i)_{1 \leq i \leq r}$ d'éléments non nuls de A tels que $(d_1 e_1, ..., d_r e_r)$ soit une base de l'image de u (avec r entier $\leq m$).
17.c. Soit $(f_1, ..., f_r) \in A^n$ tel que $u(f_i) = d e_i$. Montrer que $A^n = \ker(u) \oplus Af_1 \oplus ... \oplus Af_r$.
17.d. Montrer que la famille $(f_1, ..., f_r) \in A^n$ peut être complétée en une base $(f_1, ..., f_n)$ de A^n.

17.e. En déduire que B est équivalente à une matrice-bloc de la forme $\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$, où D est la matrice diagonale $(d_1, d_2, ..., d_r)$.
17.f. Supposons que $n = m$. En déduire le déterminant de u.
17.g. Supposons que $n = m$ et $A = \mathbf{Z}$. Montrer que le conoyau de u est fini si et seulement si $\det(u) \neq 0$. Montrer que, dans ce cas, le conoyau de u a pour ordre $|\det(u)|$.
17.h. Montrer que r est le rang de la matrice B vue comme matrice à coefficients dans le corps des fractions de A.

18. Soit S un ensemble fini de nombres premiers. Notons $\mathbf{Z}_S$ l'ensemble des nombres rationnels dont le dénominateur n'est divisible par aucun nombre premier en dehors de S.
18.a. Montrer que $\mathbf{Z}_S$ est un anneau (l'anneau des *S-entiers*).
18.b. Montrer que le groupe $\mathbf{Z}_S^\times$ est de type fini.
18.c. Est-il libre ? Quel est son rang ?
18.d. Le groupe $\mathbf{Q}^\times$ est-il de type fini ?

19. Soit p un nombre premier. Soit S un ensemble de polynômes irréductibles et unitaires sur le corps à p éléments $\mathbf{F}_p$. Notons $\mathbf{F}_p[X]_S$ l'ensemble des éléments de $\mathbf{F}_p[X]$ dont le dénominateur n'est divisible par aucun polynôme irréductible unitaire en dehors de S.
19.a. Montrer que $\mathbf{F}_p[X]_S$ est un anneau.
19.b. Montrer que le groupe $\mathbf{F}_p[X]_S^\times$ est de type fini.
19.c. Est-il libre ? Quel est son rang ? Quels sont ses éléments de torsion ?

20. Posons $\mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2}/a, b \in \mathbf{Z}\}$.
20.a. Montrer que c'est un anneau.
20.b. Montrer que le groupe des éléments inversibles est un groupe de type fini. On en donnera un système de générateurs, puis le rang et les éléments de torsion.

21. Posons $\mathbf{Z}[i] = \{a + bi \in \mathbf{C}/a, b \in \mathbf{Z}\}$ (l'anneau des *entiers de Gauss*).
21.a. Déterminer $\mathbf{Z}[i]^\times$.
21.b. Quels sont les éléments de torsion de $\mathbf{Z}[i]^\times$?

22. Soit K un corps. Posons $A = K[X]$. On considère $K(X)$ comme un A-module.
22.a. Montrer que $M = K(X)/A$ est un A-module de torsion.
22.b. Pour P polynôme irréductible unitaire de degré d, notons M_P la partie P-primaire de M. Montrer que tout élément de M_P est de la forme Q/P^n, avec $Q \in A$ et n entier ≥ 0. . En déduire que tout élément de M_P sécrit de façon unique sous la forme $\sum_i Q_i P^i$ où $Q_i \in A$ est de degré $< d$.
22.c. Montrer que pour tout élément $F \in K(X)$, il existe $E \in A$ et, pour tout $P \in A$ irréductible unitaire, une suite $(Q_{P,i})_{i \geq 0}$ (identiquement nulle pour presque tout P, et presque nulle pour tout P) avec $Q_{P,i}$ de degré $<$ degré de P. telle que $F = E + \sum_P \sum_i Q_{P,i}/P^i$.

23. Soit A un anneau principal. Soit n un entier ≥ 0. Soit M et N deux sous-A-modules de A^n. Montrer qu'il existe un automorphisme de A^n qui envoient M sur N si et seulement si A^n/M et A^n/N ont les mêmes facteurs invariants.

24. Soit A un anneau principal. Soient M et N deux A-modules de types finis. Montrer que l'ensemble des morphismes de A-modules de M vers N est un A-module de type fini.

25. Donner un exemple d'anneau factoriel A et d'un A-module M de type fini et sans torsion qui n'est pas libre. On pourra considérer $A = K[X, Y]$, avec K corps.

26. Un module M sur un anneau commutatif A est dit *simple* s'il ne contient pas d'autres sous-module que M et 0.
26.a. Soit I un idéal de A. Montrer que A/I est simple si et seulement si I est maximal.
26.b. Montrer que tout A-module simple est isomorphe à A/I, avec I idéal maximal de A. Quels sont les modules simples sur un corps ?
26.c. Montrer que tout morphisme de A-modules entre des modules simples est soit nul, soit un isomorphisme.

26.d. Montrer que les endomorphismes d'un module M constituent un anneau (non nécessairement commutatif) noté $\mathrm{End}(M)$. Lorsque M est simple, montrer que $\mathrm{End}(M)$ est une algèbre à division (un anneau dans lequel tout élément est inversible).

27. Soit K un corps. Soit n un entier ≥ 0. Notons $A = K[[X_1, X_2, ..., X_n]]$ l'ensemble des séries formelles en n indéterminées à coefficients dans K.
27.a. Montrer que $K[[X]]$ est un anneau local (c'est-à-dire qu'il possède un unique idéal maximal) et principal. Notons I l'idéal maximal de A.
27.b. Montrer que A est un anneau local dont l'unique idéal maximal est engendré par $(X_1, ..., X_n)$. Est-il principal ?
27.c. Supposons que $n = 1$. Montrer que pour tout A-module de type fini M, il existe un entier $r \geq 0$ et une suite finie décroissante d'entiers $(k_i)_{1 \leq i \leq s}$ telle que M soit isomorphe à $A^r \times A/I^{k_1} \times ... \times A/I^{k_s}$.
27.d. Montrer que ce n'est pas le cas pour $n > 1$. On pourra considérer l'idéal engendré par (X_1, X_2).

28. Soit A un anneau. Soit M un A-module. La *longueur* de M comme A-module est la borne supérieure (éventuellement ∞) de l'ensemble des entiers n tels qu'il existe une suite strictement croissante $(M_i)_{0 \leq i \leq n}$ de sous-modules de M. On la note $l(M)$.
28.a. Quelle est la longueur de M si A est un corps ?
28.b. Quelle est la longueur de $\mathbf{Z}$?
28.c. Soit n un entier. Quelle est la longueur de $\mathbf{Z}/n\mathbf{Z}$?
28.d. Quelle est la longueur d'un $\mathbf{Z}$-module de torsion de type fini en fonction de ses facteurs invariants ?

29. 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.
29.a. Montrer que $K[u] \subset L(u)$.
29.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.
29.c. Montrer que l'anneau $K[u]$ est isomorphe à $K[X]/(P)$, où P est le polynôme minimal de u.
29.d. Montrer que $L(u)$ est un K-espace vectoriel isomorphe à $\prod_{i=1}^r \mathrm{Ker}(P_i(u))$ par $\phi : v \mapsto (v(x_i))_{1 \leq i \leq r}$.
29.e. Montrer que pour tout i le projecteur sur E_i parallèlement à $\oplus_{j \neq i} E_j$ est dans $L(u)$.
29.f. Soit $w \in L(L(u))$. Montrer qu'il existe $R \in K[X]$ tel que $w(x_r) = R(u)x_r$.
29.g. Soit $v \in L(u)$ image réciproque de $(x_1, x_2...x_{r-1}, x_i)$ par ϕ. Montrer que $w(x_i) = R(u)x_i$.
29.h. Posons $L(L(u)) = \cap_{v \in L(u)} L(v)$. C'est le *bicommutant* de u. Montrer que $L(L(u)) = K[u]$.
29.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.

30. Soit B un anneau commutatif et A un sous-anneau noethérien de B. On dit que $b \in B$ est *entier* sur A si b est racine d'un polynôme unitaire de $A[X]$. On dit que B est *entier* sur A si tout élément de B est entier sur A.
30.a. Montrer que b est entier sur A si et seulement si $A[b]$ est un A-module de type fini.
30.b. En déduire que l'ensemble des éléments de B entiers sur A est un anneau, qu'on appelle *clôture intégrale* de A dans B.
30.c. Montrer que si un anneau commutatif C contenant B est entier sur B et que B est entier sur A, C est entier sur A.
30.d. Montrer que les racines de l'unités dans $\mathbf{C}$ sont entières sur $\mathbf{Z}$. Notons $\bar{\mathbf{Z}}$ l'ensemble des nombres complexes qui sont entiers sur $\mathbf{Z}$. Montrer que $\bar{\mathbf{Z}}^\times$ n'est pas un groupe de type fini.
30.e. Soit K un corps contenant $\mathbf{Q}$. Soit $\mathcal{O}_K$ l'ensemble des éléments de K entiers sur $\mathbf{Z}$. Montrer que l'ensemble des éléments de K entiers sur $\mathcal{O}_K$ est $\mathcal{O}_K$.
30.f. Montrer que tout élément de $\mathcal{O}_K^\times$ est racine d'un polynôme unitaire de coefficient constant égal à 1 ou -1.
30.g. Montrer que la partie de torsion de $\mathcal{O}_K^\times$ est cyclique.
30.h. Le groupe $\mathcal{O}_K^\times$ est-il de type fini ?