Université Rennes 1, Année 2012-2013
Master 1 Math., Algèbre générale de base

Feuille d'exercices 4

Modules

Exercice 1 - Parties génératrices minimales
Pour tout entier $n \geq 1$, trouver une partie génératrice minimale de cardinal n du $\mathbb{Z}$-module $\mathbb{Z}$.

Exercice 2 - Modules par générateurs et relations
(1) Montrez que tout A-module admet une partie génératrice. En déduire que tout A-module est isomorphe à un quotient d'un A-module libre.

(2) Montrez que $\mathbb{Z}/2\mathbb{Z}$ n'est pas isomorphe à un sous-$\mathbb{Z}$-module d'un $\mathbb{Z}$-module libre.

(3) Soit M un A-module. On appelle *présentation par générateurs et relations* de M la donnée d'une famille de générateurs $\{x_i\}_{i\in I}$ de M et d'une famille de générateurs $\{r_j\}_{j\in J}$ du noyau du morphisme $A^{(I)} \to M$, $e_i \mapsto x_i$. Pour $A = \mathbb{Z}[X]$, donnez une présentation par générateurs et relations du A-module $I = (2, X) \subset A$.

Exercice 3 - Modules sur un anneau intègre versus espaces vectoriels
Soient A un anneau commutatif intègre, et K son corps des fractions (de sorte que A est un sous-anneau de K, et que tout élément de K est un quotient d'éléments de A).

(1) Soit V un K-espace vectoriel. Montrez qu'une famille $(v_i)_{i\in I}$ d'éléments de V est libre si et seulement si elle est A-libre (i.e. libre dans V vu comme A-module).

(2) Avec les notations ci-dessus, montrez que toute famille A-génératrice dans V est K-génératrice, mais que la réciproque est fausse.

(3) Montrez que K est un A-module libre si et seulement si $A = K$.

(4) Montrez que K est un A-module de type fini si et seulement si $A = K$.

(5) Soient V et W deux K-espaces vectoriels. Montrez que toute application A-linéaire de V dans W est K-linéaire.

Exercice 4 - Modules libres versus sommes, produits, quotients, sous-modules
(1) Montrez que toute somme directe de A-modules libres est libre, et que tout produit *fini* de A-modules libres est libre. (On peut montrer que le $\mathbb{Z}$-module $\mathbb{Z}^{\mathbb{N}}$ n'est pas libre).

(2) Soient M un A-module et N un sous-module de M. Si N et M/N sont libres, montrez que M est libre.

(3) Soit $A = \mathbb{Z}/6\mathbb{Z}$. Montrez que $2A$ et $3A$ ne sont pas libres, mais que $2A \oplus 3A$ est libre de rang 1.

Exercice 5 - Faits de base sur les modules de type fini
On rappelle qu'un A-module M est dit *de type fini* s'il admet une partie génératrice finie.

(1) Montrez qu'un A-module M est de type fini si et seulement si il existe $n \in \mathbb{N}$ tel que M soit isomorphe à un quotient de A^n.

(2) Montrez que tout quotient d'un A-module de type fini est de type fini.

(3) Soit M un A-module de type fini. Montrez que toute partie génératrice de M contient une partie génératrice finie.

(4) Dans l'anneau $\mathbb{Z}^{\mathbb{N}}$, montrez que $\mathbb{Z}^{(\mathbb{N})}$ est un idéal qui n'est pas de type fini.

(5) Donnez un exemple d'un sous-module d'un module de type fini qui n'est pas de type fini.

(6) Montrez qu'un A-module libre est de type fini si et seulement si il est de rang fini (i.e. isomorphe à A^n pour un $n \in \mathbb{N}$).

(7) Soient M un A-module et N un sous-module de M. Montrez que si N et M/N sont de type fini, M est de type fini.

Exercice 6 - Générateurs des rationnels
$\mathbb{Q}$ est ici considéré comme un $\mathbb{Z}$-module.

(1) Montrer que tout sous-module de type fini de $\mathbb{Q}$ est libre de rang 0 ou 1. En déduire que $\mathbb{Q}$ n'est pas de type fini, puis (en utilisant l'exercice précédent) la même chose pour $\mathbb{Q}/\mathbb{Z}$.

(2) Soit $(e_i)_{i \in I}$ une famille génératrice de $\mathbb{Q}$ et $j \in I$. Montrer que la famille $(e_i)_{i \in I \setminus \{j\}}$ est encore génératrice.

Exercice 7 - Deux faits sur les modules de torsion de type fini
Soient A un anneau commutatif intègre, et M un A-module. On dit que $x \in M$ est *de torsion* s'il existe $a \in A$, $a \neq 0$, tel que $ax = 0$. On dit que M est *de torsion* si tous ses éléments sont de torsion.

(1) On suppose M de type fini. Montrez que M est de torsion si et seulement si $\mathrm{Ann}(M)$ est non nul.

(2) On suppose que $A = \mathbb{Z}$. Montrez que M est de torsion et de type fini si, et seulement si, M est fini.

Anneaux intègres, factoriels, principaux

Exercice 8 - Algèbres par générateurs et relations
(1) Montrez que toute A-algèbre admet une partie génératrice. En déduire que toute A-algèbre est isomorphe à un quotient d'une A-algèbre de polynômes (en un nombre arbitraire de variables).

(2) Montrez que $\mathbb{Z}/2\mathbb{Z}$ n'est pas isomorphe à une sous-$\mathbb{Z}$-algèbre d'une $\mathbb{Z}$-algèbre de polynômes.

(3) Soit B une A-algèbre. On appelle *présentation par générateurs et relations* de B la donnée d'une famille de générateurs $\{x_i\}_{i \in I}$ de B et d'une famille de générateurs $\{y_j\}_{j \in J}$ du noyau du morphisme $A[X_i]_{i \in I} \to B$, $X_i \mapsto x_i$. Pour A égale à un corps k, donnez une présentation par générateurs et relations de la k-algèbre des polynômes en une variable X à coefficients dans k sans terme de degré 1.

Exercice 9 - **Principalité de $A[X]$**
Soit A un anneau commutatif. Montrer que l'anneau $A[X]$ est principal si et seulement si A est un corps.

Exercice 10 - **Formules pour pgcd et ppcm**
Soit A un anneau factoriel et $a, b, \ldots$ des éléments de A.

(1) Montrez que $\mathrm{pgcd}(a, \mathrm{pgcd}(b, c)) = \mathrm{pgcd}(a, b, c)$.

(2) Montrez que $\mathrm{pgcd}(a^n, b^n) = \mathrm{pgcd}(a, b)^n$ pour tout entier $n \geq 1$.

(3) Montrez que $\mathrm{pgcd}(a, b)\mathrm{ppcm}(a, b) = ab$.

(4) Montrez que $\mathrm{pgcd}(a, \mathrm{ppcm}(b, c)) = \mathrm{ppcm}(\mathrm{pgcd}(a, b), \mathrm{pgcd}(a, c))$.

(5) Montrez que $\mathrm{ppcm}(a, \mathrm{pgcd}(b, c)) = \mathrm{pgcd}(\mathrm{ppcm}(a, b), \mathrm{ppcm}(a, c))$.

(6) Si $A = \mathbb{Z}$ montrez que $\mathrm{pgcd}(a, b) = \sum_{k|a, k|b} \varphi(k)$ où φ est la fonction indicatrice d'Euler.

(7) Si A est euclidien de stathme δ, montrez que pour toute division euclidienne $a = bq + r$ avec $\delta(r) < \delta(b)$ on a $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r)$.

(8) Si $A = \mathbb{Z}$ montrez que $\mathrm{pgcd}(n^a - 1, n^b - 1) = n^{\mathrm{pgcd}(a,b)} - 1$.

(9) Si $A = k[X]$ où k est un corps, montrez que $\mathrm{pgcd}(X^a - 1, X^b - 1) = X^{\mathrm{pgcd}(a,b)} - 1$.

Exercice 11 - **Entiers de Gauss**
Soit $A = \mathbb{Z} + i\mathbb{Z} \subset \mathbb{C}$.

(1) Montrez que A est un sous-anneau de $\mathbb{C}$, et un $\mathbb{Z}$-module libre de rang 2. Montrer que la conjugaison complexe est un automorphisme d'anneau de A.

(2) On définit la *norme* $N : A \to \mathbb{N}$ par $N(z) = |z|^2$. Quels sont les éléments de norme 1 de A ? Quels sont les inversibles de A ?

(3) Montrez que N est un stathme euclidien sur A. (Indication : montrer que pour tout $u \in \mathbb{C}$, il existe $z \in A$ tel que $|u - z| < 1$. On suggère de faire un dessin.)

(4) Montrer que $1 + i$ et $1 + 2i$ sont irréductibles dans A (regarder les normes) et que 2 et 5 ne le sont pas.

(5) Soit p un nombre premier. On considère les conditions suivantes:

- (i) p n'est pas irréductible dans A;
- (ii) p est somme de deux carrés d'entiers;
- (iii) $p = 2$ ou $p \equiv 1 \pmod 4$.

Montrer que (i) $\Leftrightarrow$ (ii) $\Rightarrow$ (iii).

(6) (Plus difficile) Montrer que l'on a aussi (iii) $\Rightarrow$ (i) dans la question précédente. (Indication : si p est irréductible dans A, alors l'équation $x^2 + 1 = 0$ admet dans le corps A/pA une solution qui n'est pas dans $\mathbb{Z}/p\mathbb{Z}$. En déduire que -1 n'est pas un carré modulo p, donc que $p \equiv -1 \pmod 4$.)

Exercice 12 - Contre-exemples

Soit k un corps et soit A le sous-anneau de $k[X]$ formé des polynômes sans terme en X (c'est donc le sous-k-espace vectoriel de $k[X]$ engendré par les X^i ($i \in \mathbb{N}$, $i \neq 1$).

(1) Est-ce bien un sous-anneau de $k[X]$? Quels sont ses éléments inversibles ?

(2) Pour chaque entier $m \geqslant 2$, décrire l'ensemble des diviseurs de X^m dans A, et l'ensemble de ses multiples de la forme X^n ($n \in \mathbb{N}$). Quels sont les X^m qui sont irréductibles dans A ? Lesquels sont premiers ?

(3) L'idéal (X^2, X^3) de A est-il principal ?

(4) Pour quelles valeurs de m le couple (X^m, X^{m+1}) admet-il un pgcd (resp. un ppcm) dans A ?

(5) Que donne la formule d'associativité $\mathrm{pgcd}(a, \mathrm{pgcd}(b, c)) = \mathrm{pgcd}(a, b, c)$ avec $a = X^2$, $b = X^5$ et $c = X^6$? Que donne la formule d'homogénéité $\mathrm{pgcd}(ca, cb) = c\mathrm{pgcd}(a, b)$ avec $a = X^2$, $b = X^3$ et $c = X^3$?

(6) Trouver deux écritures non équivalentes de X^6 comme produit d'irréductibles.