Feuille d'exercices
Anneaux

Exercice 1 (Double quotient d'un anneau).

Soit A un anneau et I, J deux idéaux de A.

(a) On note $\pi_I : A \to A/I$ et $\pi_J : A \to A/J$ les projections canoniques. Montrer que $(A/I)/\pi_I(J)$ et $(A/J)/\pi_J(I)$ sont canoniquement isomorphes.

(b) Soit $P \in \mathbb{Z}[X]$ unitaire irréductible et α une racine de P dans $\mathbb{C}$. Donner un critère pour qu'un nombre premier p soit toujours premier dans $\mathbb{Z}[\alpha]$.

(c) Pour un entier $n \geq 3$, montrer que 2 est toujours irréductible dans $\mathbb{Z}[i\sqrt{n}]$. En déduire (par disjonction des cas pair et impair) que $\mathbb{Z}[i\sqrt{n}]$ n'est pas factoriel.

Exercice 2 (Questions diverses).

(a) Montrer que si $A[X]$ est un anneau principal alors A est un corps.

(b) Plus généralement, parmi les propriétés euclidien/principal/factoriel/noethérien, lesquelles sont stables par sous-anneau ou anneau quotient ?

Exercice 3 (Anneaux d'entiers quadratiques).

Soit $d \neq 0, 1$ un entier sans facteur carré. On note $\sqrt{d}$ un choix de racine carrée de d (imaginaire pur si $d < 0$), $K = \mathbb{Q}(\sqrt{d})$ et $\mathcal{O}_K$ l'ensemble des entiers algébriques de K.

(a) Si $d \equiv 2, 3 \mod 4$, montrer que $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.

(b) Si $d \equiv 1 \mod 4$, montrer que $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ et trouver le polynôme minimal sur $\mathbb{Z}$ de cet élément.

(c) Supposons que $d < 0$. Montrer que $N : z \mapsto |z|^2$ est à valeurs entières sur $\mathcal{O}_K$, et que c'est un stathme euclidien pour $\mathcal{O}_K$ si et seulement si $d \in \{-1, -2, -3, -7, -11\}$.

(d) Trouver les inversibles de $\mathcal{O}_K$ pour tout $d < 0$.

(e) Déterminer les irréductibles de $\mathbb{Z}[i]$ (en utilisant qu'il est euclidien), et en déduire quels nombres premiers s'écrivent comme somme de deux carrés d'entiers.

(f) Montrer que $\mathbb{Z}[\sqrt{2}]$ a une infinité d'inversibles.

Exercice 4 (Lemme des noyaux). Soit K un corps, E un K-espace vectoriel de dimension finie, u un endomorphisme de E et $P \in K[X]$ un polynôme annulateur de u.

(a) Montrer que si $P = QR$ avec $Q, R \in K[X]$ premiers entre eux, alors

$$E = \operatorname{Ker} Q \oplus \operatorname{Ker} R$$

et que les projections selon cette décomposition sont des polynômes en u.

(b) Si K est algébriquement clos, en déduire la décomposition de Dunford, c'est-à-dire que tout endomorphisme de E s'écrit de manière unique comme

$$u = d + n$$

avec d diagonalisable et n nilpotent (et ils sont tous les deux des polynômes en u).

Exercice 5 (Exemple d'équation de Mordell).

Dans cet exercice, on cherche à résoudre dans $\mathbb{Z}$ l'équation de Mordell

$$y^2 = x^3 - 2.$$

(a) Rappeler pourquoi $\mathbb{Z}[i\sqrt{2}]$ est factoriel.

(*b*) Pour A un anneau factoriel et $a, b \in A$ premiers entre eux tels que $ab = c^n$ pour un certain $n \geq 1$, montrer qu'il existe $u, v \in A^*$ et $\alpha, \beta \in A$ tels que $a = u\alpha^n$ et $b = v\beta^n$.

(*c*) Soit (x, y) une solution de l'équation de Mordell. Montrer que $(y + i\sqrt{2})$ et $(y - i\sqrt{2})$ sont premiers entre eux dans $\mathbb{Z}[i\sqrt{2}]$ puis que ce sont des cubes dans cet anneau.

(*d*) En écrivant explicitement le fait d'être un cube, en déduire que les seules solutions de l'équation dans $\mathbb{Z}$ sont $(3, 5)$ et $(3, -5)$.

Exercice 6 (Critère d'Eisenstein)**.**

(*a*) Soit $n \geq 2$ et K un corps de caractéristique différente de 2. Montrer par récurrence que

$$X_1^2 + \cdots + X_n^2 - 1$$

est irréductible dans $K[X_1, \cdots, X_n]$. Que se passe-t'il en caractéristique 2 ?

(*b*) Soit $n \geq 2$ et K un corps de caractéristique première à n. Montrer que $X^n + Y^n - 1$ est irréductible sur $K[X, Y]$.

Exercice 7 (Anneaux non factoriels)**.**

(*a*) Montrer que pour un corps K quelconque, $K[X^2, X^3] \subset K[X]$ n'est pas factoriel malgré l'existence d'une décomposition en irréductibles. Que peut-on même remarquer sur cette décomposition en irréductibles ?

Soit $\mathcal{H}(\mathbb{C})$ l'anneau des fonctions entières sur $\mathbb{C}$.

(*b*) Montrer que $\mathcal{H}(\mathbb{C})$ est intègre, et trouver ses inversibles.

(*c*) Montrer que les irréductibles de $\mathcal{H}(\mathbb{C})$ sont à inversible près les fonctions affines $z \mapsto z - z_0$, $z_0 \in \mathbb{C}$.

(*d*) En déduire que $\mathcal{H}(\mathbb{C})$ n'est pas factoriel ni noethérien.

Exercice 8 (Contre-exemples sur les modules)**.**

(*a*) Donner un exemple de A-module de type fini mais pas libre.

(*b*) Donner un exemple de A-module (libre) de type fini qui admette un sous A-module qui n'est pas de type fini.

(*c*) Donner un exemple de sous-A-module d'un A-module qui n'admette pas de supplémentaire.

Exercice 9 (Théorème des diviseurs élémentaires)**.**

Soit A un anneau principal.

Pour $n \geq 2$ et $1 \leq i < j \leq n$, une transvection généralisée (terme *ad hoc*) est une matrice de $M_n(A)$ égale à l'identité à part le bloc 2×2 d'indices (i, j), sur lequel c'est une matrice de $\mathrm{SL}_2(A)$.

Soit M une matrice de $M_{m,n}(A)$.

(*a*) Pour $k \leq \min(m, n)$, on note $D_k(M)$ le pgcd des mineurs de taille k de M. Montrer que $D_k(M) = D_k(M')$ si M et M' sont équivalentes dans A.

En déduire que les diviseurs élémentaires, s'ils existent, sont bien définis à inversibles près.

(*b*) Montrer qu'il suffit de prouver que toute matrice M est équivalente à une matrice de la forme

$$\begin{pmatrix} D_1(M) & 0 \\ 0 & M' \end{pmatrix}$$

avec M' de taille $m - 1, n - 1$ et dont tous les coefficients sont divisibles par $D_1(M)$.

(*c*) Montrer qu'en multipliant par des matrices de transvection généralisées à droite et à gauche, on peut obtenir que m_{11} divise tous les éléments de la première ligne et la première colonne de M.

(*d*) Si $(m_{11}) = (D_1(M))$, conclure.

(*e*) Si $(m_{11}) \neq (D_1(M))$, montrer qu'il existe une matrice $M^{(2)}$ équivalente à M telle que $m_{11}^{(2)}$ divise strictement m_{11}. Expliquer pourquoi le procédé doit s'arrêter et conclure.

Exercice 10 (Applications des diviseurs élémentaires).

(*a*) Trouver les diviseurs élémentaires de la matrice

$$\begin{pmatrix} 1 & 0 & -1 & 3 \\ 4 & 5 & 2 & -1 \\ 3 & 7 & 0 & 2 \end{pmatrix} \in M_{3,4}(\mathbb{Z}).$$

(*b*) Trouver la structure canonique des groupes abéliens donnés par générateurs et relations suivants :

G_1 engendré par x, y et z tels que $15x = 0$, $x + y + z = 0$ et $3x + 8y = 0$.

G_2 engendré par x, y et z tels que

$$\begin{cases} 2x - y - 3z & = & 0 \\ 3x - 2y - 3z & = & 0 \\ 7x + 4y + 10z & = & 0 \end{cases}$$

Exercice 11 (Invariants de similitude).

Soit E un K-espace vectoriel de dimension finie et u un endomorphisme de E.

(*a*) En considérant E comme un $K[X]$-module via $P \cdot x = P(u)(x)$, montrer qu'il existe des polynômes unitaires $P_1 | \cdots | P_r$ tels qu'en tant que $K[X]$-module,

$$E \cong K[X]/(P_1) \times \cdots \times K[X]/(P_r).$$

(*b*) En déduire une base de E dans laquelle la matrice de u est de la forme

$$M = \begin{pmatrix} C_{P_1} & & \\ & \ddots & \\ & & C_{P_r} \end{pmatrix}$$

où pour un polynôme P, C_P est sa matrice compagnon.

(*c*) Montrer que P_r est le polynôme minimal de u, $P_1 \cdots P_r$ son polynôme caractéristique, et que $P_1, \cdots, P_r$ caractérisent les classes de similitude de $M_n(K)$. En déduire que si deux matrices de $M_n(K)$ sont semblables dans une extension de K, elles le sont dans $M_n(K)$.

(*d*) Montrer qu'aux facteurs constants près, $P_1, \cdots, P_r$ est la suite des diviseurs élémentaires de la matrice $XI_n - M \in M_n(K[X])$. En déduire un algorithme pour calculer les invariants de similitude d'un endomorphisme.