Université de Rennes 1 - UFR Mathématiques - Année 2011-2012
Master 1 de mathématiques - Algèbre générale de base

Évaluation des exercices :

[E]= « élémentaire » : application directe des définitions et des résultats du cours.
[S]= « standard » : exercice « classique », souvent rencontré et souvent utilisé.

Feuille d'exercices 5

Par défaut, les anneaux sont commutatifs et A désigne un anneau.

[E] **Exercice 1 -** Soient M un A-module de type fini (feuille 4, ex. 13) et $\underline{v} = (v_1, \ldots, v_n)$ une famille génératrice de M. Si f est un endomorphisme de M, on dira que $U = (u_{i,j})_{1 \leq i \leq n, 1 \leq i \leq n} \in \mathrm{M}_n(A)$ est *une* matrice de f par rapport à $\underline{v}$ si l'on a

$$\forall j \in \{1, \ldots, n\}, \quad f(v_j) = \sum_{i=1}^{n} u_{i,j} v_i.$$

1 - Montrer que tout endomorphisme de M admet (au moins) une matrice, et qu'il est déterminé par celle-ci.

2 - Si U (resp. V) est une matrice de f (resp. g), montrer que $\lambda U + \mu V$ est une matrice de $\lambda f + \mu g$ ($\lambda, \mu \in A$) et que UV est une matrice de $f \circ g$. En déduire que, pour tout $P \in A[T]$, $P(U)$ est une matrice de $P(f)$.

3 - Montrer que pour tout $f \in \mathrm{End}(M)$ il existe $P \in A[T]$ unitaire tel que $P(f) = 0$.

Exercice 2 - (« lemme de Nakayama ») Soient M un A-module de type fini et I un idéal de A tel que $IM = M$. Montrer qu'il existe $x \in 1 + I$ tel que $xM = 0$.

Exercice 3 - (éléments entiers sur un anneau) Soit A un sous-anneau d'un anneau B, et soit z un élément de B.

[E] **1 -** Notons $\mu_b : B \to B$ la multiplication par b, vue comme endomorphisme du A-module B. Pour tout $P \in A[T]$, montrer que $P(\mu_b) = \mu_{P(b)}$.

[ES] **2 -** On note $A[z] \subset B$ le sous-anneau de B engendré par A et z. Montrer que $A[z]$ est le sous-A-module de B engendré par la famille $(z^n)_{n \in \mathbb{N}}$.

[S] **3 -** Montrer que les conditions suivantes sont équivalentes :

(i) z est « entier sur A » : il existe $P \in A[T]$ *unitaire* tel que $P(z) = 0$;
(ii) $A[z]$ est un A-module de type fini ;
(iii) il existe un sous-anneau $C \subset B$ contenant $A[z]$ et qui est un A-module de type fini.

(Indication : pour (iii)$\Rightarrow$ (i), utiliser l'exercice **1** et la question **1**).

[S] **4 -** Soient x et y dans B, tous deux entiers sur A. Montrer que le sous-anneau $A[x, y]$ de B engendré par A, x et y est un A-module de type fini. (Considérer les « monômes » $x^i y^j$).

[S] **5 -** En déduire que $\{z \in B \mid z \text{ est entier sur } A\}$ est un sous-anneau de B.

Divisiblité, anneaux principaux

[E] **Exercice 4 -** Soit A un anneau intègre.

1 - Montrer que la relation « x divise y » dans A (resp. dans A^*) est une relation de préordre (réflexive et transitive) compatible avec la multiplication. À quelle condition est-ce une relation d'ordre ? Que dire de la relation induite par passage au quotient sur $A/\sim$?

2 - Si x, y, c sont trois éléments de A, discuter l'équivalence $x|y \Leftrightarrow cx|cy$.

Exercice 5 - Soit A un anneau intègre. Dans ce qui suit les égalités faisant intervenir des PGCD et PPCM doivent être comprises dans $A/\sim$.

[E] **1 -** (associativité du PGCD et du PPCM) Montrer la formule $\mathrm{PGCD}(a, \mathrm{PGCD}(b, c)) = \mathrm{PGCD}(a, b, c)$ au sens suivant : si le *premier* membre existe, alors c'est un PGCD de (a, b, c). Question analogue pour le PPCM.

[E] **2 -** (homogénéité du PGCD et du PPCM) Montrer la formule $\mathrm{PGCD}(ac, bc) = c\,\mathrm{PGCD}(a, b)$, avec le même sens que précédemment, et où c est supposé non nul. Question analogue pour le PPCM.

3 - (PGCD, PPCM et produit) Soient a et b non nuls dans A. Montrer que l'application $x \mapsto ab/x$ est une bijection entre l'ensemble des diviseurs communs de a et b et l'ensemble des multiples communs de a et b qui divisent ab. En déduire que si a et b ont un PPCM m, alors ils ont un PGCD (à savoir ab/m).

Exercice 6 - On suppose A principal (ou seulement factoriel), et l'on note K son corps des fractions.

[ES] **1 -** Refaire l'exercice **5**.

[S] **2 -** (« lemme de Gauss ») Montrer que si $a|bc$ et $\mathrm{PGCD}(a, b) = 1$, alors $a|c$, de deux manières : par décomposition en irréductibles, et (si A est principal) par l'identité de Bézout.

3 - Soient a et b dans A et $m, n \in \mathbb{N}$. Montrer que $\mathrm{PGCD}(a^n, b^n) = \mathrm{PGCD}(a, b)^n$. Montrer que si a et b sont premiers entre eux, alors a^m et b^n sont premiers entre eux.

[S] **4 -** Montrer que tout élément z de K s'écrit sous la forme « irréductible » $z = \frac{a}{b}$ avec $a \in A$, $b \in A^*$ et $\mathrm{PGCD}(a, b) = 1$. Montrer que si a' et b' vérifient les mêmes conditions, alors il existe $\varepsilon \in A^\times$ tel que $a' = \varepsilon\, a$ et $b' = \varepsilon\, b$.

5 - Soient x un élément de A et $n \in \mathbb{N}$. Montrer que si x est une puissance n-ième dans K, c'est une puissance n-ième dans A. (Pour une généralisation, voir l'exercice **9**). Qu'obtient-on pour $A = \mathbb{Z}$, $n = 2$ et $x = 2$?

[S] **Exercice 7 -** (Entiers de Gauss) Soit $A = \mathbb{Z} + i\mathbb{Z} \subset \mathbb{C}$.

[ES] **1 -** Montrer 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.

[S] **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 ?

[S] **3 -** Montrer que N est une jauge euclidienne 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.

[S] **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).

[S] **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 $p \equiv -1 \pmod 4$.]

[S] **Exercice 8 -** On note j le nombre complexe $\frac{1+i\sqrt{3}}{2}$. On rappelle que $1+j+j^2=0$ et que $j^3=1$. On pose $A = \mathbb{Z} + j\,\mathbb{Z} \subset \mathbb{C}$. Refaire pour A les questions 1 à 3 de l'exercice **7**.

[S] **Exercice 9 -** (Racines de polynômes sur un anneau factoriel). Soient A un anneau factoriel et K son corps des fractions. Soit $P \in A[X]$ de la forme $P = \sum_{i=0}^{d} a_i X^i$ ($a_i \in A$, $a_d \neq 0$). On suppose que $\mathrm{PGCD}(a_0, \ldots, a_d) = 1$.

[E] **1 -** Soit x une racine de P dans K. On écrit $x = u/v$ avec $u \in A$, $v \in A^*$, $\mathrm{PGCD}(u,v) = 1$ (cf. exercice **6**). Montrer que $v|a_d$ et que $u|a_0$ (utiliser le lemme de Gauss).

[E] **2 -** En déduire que tout élément de K entier sur A (exercice **3**) appartient à A.

3 - Trouver les racines rationnelles du polynôme $3X^4 - 2X^3 - 6X + 4$. Même question pour $X^{51} - 7^{39}X^{48} + 18X^9 - 1440X^8 + 1$.

Exercice 10 - Soit d un entier qui n'est pas un carré. On pose $\delta = \sqrt{d}$ si $d > 0$ et $\delta = i\sqrt{-d}$ si $d < 0$. Soit $A = \mathbb{Z} + \delta\mathbb{Z} \subset \mathbb{C}$.

1 - Montrer que A est un $\mathbb{Z}$-module libre de rang 2 et un sous-anneau de $\mathbb{C}$ (aussi noté $\mathbb{Z}[\delta]$).

2 - On suppose que d « a un facteur carré » : $d = ab^2$ avec a et b entiers, $b \geq 2$. Déduire de l'exercice **9** que A n'est pas factoriel. (Considérer δ/b).

3 - On suppose que $d \equiv 1 \pmod 4$. Déduire de l'exercice **9** que A n'est pas factoriel. (Considérer $\frac{1+\delta}{2}$).

4 - Peut-on appliquer les questions **2** et **3** à l'anneau $\mathbb{Z}[i\sqrt{5}]$? Montrer qu'il n'est pas factoriel en calculant $(1+i\sqrt{5})(1-i\sqrt{5})$.

[S] **Exercice 11 -** (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 $m \geq 2$, 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 du PGCD (ex. **5**, question **1**) avec $a = X^2$, $b = X^5$ et $c = X^6$? Que donne la formule d'homogénéité du PGCD (ex. **5**, question **2**) avec $a = X^2$,

$b = X^3$ et $c = X^3$? Trouver un contre-exemple à la réciproque de la dernière assertion de l'ex. **5**, question **3**.

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

7 - Dans le corps des fractions de A (identifié à $k(X)$) montrer que tout élément admet une écriture irréductible, au sens de l'exercice **6**, question **4** (raisonner sur les degrés) mais que l'« unicité » est en défaut (considérer l'élément X).