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

Feuille d'exercices 5 : indications de solutions

Exercice 1 - 3 : prendre pour P le polynôme caractéristique de f (au signe près).

Exercice 2 - (« lemme de Nakayama ») On peut appliquer l'exercice précédent à l'endomorphisme Id_M. Le fait que $IM = M$ implique que Id_M admet une matrice U dont tous les coefficients sont dans I. Si P est le polynôme caractéristique de U, on a donc $0 = P(\mathrm{Id}_M) = x\mathrm{Id}_M$ où $x = P(1)$. Mais P est de la forme $\pm X^n +$ (polynôme à coefficients dans I), donc $P(1) \in \pm 1 + I$, d'où la conclusion.

Exercice 3 - 2 : il est clair que tout sous-anneau contenant A et z contient le sous-module en question. Vérifier que ce sous-module est bien un sous-anneau contenant A et z. **3** : (i)⇒(ii) : si $d : \deg P$, alors z^d est combinaison linéaire de $1, Z, \ldots, z^{d-1}$; il en résulte par récurrence que z^m est combinaison linéaire de $1, z, \ldots, z^{d-1}$ pour tout $m \geq d$. Donc la famille $(1, z, \ldots, z^{d-1})$ engendre le A-module $A[z]$. (iii)⇒(i) : la muliplication par z est un endomorphisme $\mu_{C,z}$ du A-module C. D'après l'exercice 1, question 3, il existe $P \in A[T]$ unitaire tel que $P(\mu_{C,z} = 0$. Donc $\mu_{C,P(z)} = 0$ (question 1) et $P(z) = \mu_{C,P(z)}(1) = 0$.
4 : si $A[x]$ est engendré comme A-module par $(1, x, \ldots, x^{d-1})$ et $A[y]$ par $(1, y, \ldots, y^{e-1})$, vérifier que $A[x, y]$ est engendré par le produits $x^i\, y^j$ $(i \leq d-1,\ j \leq e-1)$.
5 : si x et y appartiennent à B, alors $x - y$ et xy appartiennent à $C := A[x, y]$ qui est un A-module de type fini (question 4) donc ils sont entiers sur A (question 3, condition (iii)).

Exercice 4 - 1 : c'est une relation d'ordre si et seulement si $A^\times = \{1\}$. La relation induite sur $A/\sim$ est une relation d'ordre. **2** : ⇒ toujours vraie, ⇐ vraie si $c \neq 0$,

Exercice 5 - Si S est une partie de A, notons $\mathrm{Div}(S)$ l'ensemble des diviseurs communs des éléments de S.
1 : soient $d := PGCD(b, c)$ et $e := PGCD(a, d)$ (supposés exister). On a $\mathrm{Div}(e) = \mathrm{Div}(a, d) = \mathrm{Div}(a) \cap \mathrm{Div}(d) = \mathrm{Div}(a) \cap \mathrm{Div}(b, c) = \mathrm{Div}(a, b, c)$. Donc d est un PGCD de $\{a, b, c\}$. L'argument est le même pour le PPCM.
2 : soit $d = \mathrm{PGCD}(ac, bc)$, supposé exister. Alors c divise ac et bc donc divise d, et l'on peut écrire $d = cd'$ avec $d \in A$. Vérifier alors que pour tout $x \in A$, on a : $(x|d') \Leftrightarrow (x|a$ et $x|b)$ (multiplier par c et appliquer l'exercice 4). La formule $\mathrm{PPCM}(ac, bc) = c\,\mathrm{PPCM}(a, b)$ est vraie en supposant l'existence du *second* membre (démonstration analogue).

Exercice 7 - 1 : $(1, i)$ est une $\mathbb{Z}$-base de A. **2** : les éléments de norme 1 sont ± 1 et $\pm i$. Ce sont aussi les inversibles (utiliser le fait que $N(zz') = N(z)N(z')$). **3** : si $u = x + iy$ $(x, y \in \mathbb{R})$, il existe des entiers ξ et η tels que $|x - \xi| \leq 1/2$ et $|y - \eta| \leq 1/2$. L'élément $z := \xi + i\eta$ de A vérifie $|u - z| \leq 1/\sqrt{2} < 1$. Soient alors a et b dans A, avec $b \neq 0$: appliquant ce qui précède à $u = a/b$ on trouve $z \in A$ vérifiant $|a - bz| < |b|$. **4** : il est immédiat que tout élément de A dont la norme est un nombre premier est irréductible (attention aux inversibles !). Ceci s'applique à $1 + i$ et à $1 + 2i$. D'autre part, les relations $2 = (1 + i)(1 - i)$ et $5 = (1 + 2i)(1 - 2i)$ impliquent que 2 et 5 ne sont pas irréductibles.

5 : si p n'est pas irréductible, alors $p = uv$ avec u et v dans A, non inversibles et non nuls donc de norme > 1. On a donc $p^2 = N(p) = N(u)N(v)$ ce qui n'est possible que si $N(u) = N(v) = p$. Donc p est une norme, c'est-à-dire une somme de deux carrés. Réciproquement, si $p = a^2 + b^2$ alors $p = (a + ib)(a - ib)$, où $a + ib$ et $a - ib \in A$ sont tous deux de norme p, donc non inversibles. Enfin, si p est somme de deux carrés et est $\neq 2$, alors p est impair donc est somme d'un carré pair (donc $\equiv 0 \pmod 4$) et d'un carré impair (donc $\equiv 1 \pmod 4$).
6 : si p n'est pas irréductible dans A alors $p \neq 2$ (question 4) donc p est impair. L'idéal pA est maximal donc $F := A/pA$ est un corps dans lequel la classe de i est un élément de carré -1. Cet élément n'est pas la classe d'un entier (les éléments de $\mathbb{Z} + pA$ ont une partie imaginaire divisible par p). Donc, dans F, les deux solutions de l'équation $x^2 = -1$ ne sont pas dans $\mathbb{Z}/p\mathbb{Z}$, de sorte que -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$. On sait que ceci implique que $p \equiv -1 \pmod 4$.

[S] **Exercice 9 -** **1** : on a $0 = v^d\, P(u/v) = a_{d\,u^d} + \sum_{i=0}^{d-1} a_i u^i\, v^{d-i}$. Dans le second membre, la somme est divisible par v, qui est premier avec u (donc avec u^d), donc v divise a_d. **2** : appliquer la question précédente avec $a_{d=1}$. **3** : 2/3 pour le premier, aucune pour le second.

Exercice 10 - **2** : le nombre $\delta/b \in \mathrm{Frac}\,(A)$ n'appartient pas à A (pourquoi ?) et est racine du polynôme $X^2 - a$. **3** : le nombre $\frac{1+\delta}{2} \in \mathrm{Frac}\,(A)$ n'appartient pas à A et est racine du polynôme $X^2 - X - \frac{d-1}{4}$. **4** : on a $(1 + i\sqrt{5})(1 - i\sqrt{5}) = 2 \times 3$. Or 2 est irréductible dans $A := \mathbb{Z}[i\sqrt{5}]$ (car un diviseur de 2 dans A doit être de norme ≤ 4 donc entier) et ne divise aucun des facteurs du membre de gauche.

Exercice 11 - On conserve la notation Div de l'exercice **5**. On observe que a divise b dans A si et seulement si a divise b dans $k[X]$ *ET* le polynôme b/a est dans A.
1 : $A^\times = k^*$. **2** : $\mathrm{Div}(X^m)$ est l'ensemble des λX^p avec $\lambda \in k^*$ et $0 \leq p \leq m$, $p \neq 1$, $p \neq m-1$. Les multiples de X^m qui sont des puissances de X sont les X^p où $p = m$ ou $p \geq m + 2$. X^m est irréductible si et seulement si $m = 2$ ou $m = 3$. Aucun n'est premier : X^2 divise $(X^3)^2$ mais ne divise pas X^3, et X^3 divise $(X^2)^3$ mais ne divise pas X^2. **3** : la question **2** montre que X^2 et X^3 sont premiers entre eux ; si l'idéal était principal ils seraient donc étrangers. **4** : il n'y a jamais de PPCM ; pas de PGCD si $m \geq 5$; $\mathrm{PGCD}\,(X^2, X^3) = \mathrm{PGCD}\,(X^3, X^4) = 1$; $\mathrm{PGCD}\,(X^4, X^5) = X^2$. **5** : X^2 et X^3 ont un PGCD mais pas de PPCM. **6** : $(X^3)^2 = (X^2)^3$. **7** : $X = X^3/X^2 = X^4/X^3$.