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

Contrôle 2, corrigé

Exercice 1 [2 points] Soit A un anneau. Décrivez l'anneau des endomorphismes du A-module à gauche A.

[1 pt] Soit $f : A \to A$ un endomorphisme du A-module à gauche A, et posons $a_f = f(1_A)$. Pour tout $x \in A$ on a $f(x) = f(x.1_A) = x.f(1_A) = xa_f$. Ceci montre que f est déterminé par a_f. Réciproquement, pour tout $a \in A$ l'application $f_a : A \to A$ définie par $f_a(x) = xa$ est un endomorphisme du A-module A. Les applications $f \mapsto a_f$ et $f_a \hookleftarrow a$ définissent donc une bijection $\varphi : \mathrm{End}_A(A) \to A$.

[1 pt] L'application φ envoie une somme d'endomorphismes $f+g$ sur l'élément $a_{f+g} = (f+g)(1_A) = f(1_A) + g(1_A) = a_f + a_g$ donc c'est un morphisme de groupes. De plus elle envoie l'endomorphisme identité $f = \mathrm{Id}_A$ sur l'élément $a_f = 1$.

[1 pt] Enfin φ envoie fg sur l'élément $a_{fg} = (fg)(1_A) = f(g(1_A)) = f(a_g) = a_g.f(1_A) = a_g a_f$. En d'autres termes $\varphi(fg) = \varphi(g)\varphi(f)$, donc finalement φ est un morphisme de l'anneau unitaire $\mathrm{End}_A(A)$ vers l'anneau unitaire A° opposé de A. En conclusion $\mathrm{End}_A(A) \simeq A^\circ$.

Exercice 2 [2 points] Soient k un corps (commutatif), A une k-algèbre de dimension finie, $x \in A$. Montrez que si x est régulier à gauche, alors il est inversible (à droite et à gauche).

[1 pt] Si x est régulier à gauche, alors l'application $\gamma_x : A \to A$ définie par $\gamma_x(y) = xy$ est injective. Comme γ_x est k-linéaire et A est de dimension finie, alors γ_x est en fait bijective donc en particulier surjective. Alors il existe $y \in A$ tel que $xy = 1$, i.e. x possède un inverse à droite.

[1 pt] En multipliant à droite par x on trouve $xyx = x$ c'est-à-dire $\gamma_x(yx) = \gamma_x(1)$. Comme γ_x est injective, on en déduit $yx = 1$ donc y est aussi inverse à gauche pour x. Finalement x est inversible.

Exercice 3 Soit M l'ensemble des polynômes $P \in \mathbb{R}[X]$ tels que $P(\mathbb{Z}) \subset \mathbb{Z}$.

(a) [1 point] Montrez que M est un $\mathbb{Z}$-module.

(b) [2 points] On pose $H_0 = 1$ et $H_n = \frac{X(X-1)\ldots(X-n+1)}{n!}$ pour $n \geqslant 1$ entier. Montrez que $H_n \in M$.

(c) [2 points] Montrez que $\{H_n\}_{n \geqslant 0}$ est une famille libre du $\mathbb{Z}$-module M.

(d) [2 points] Montrez que $\{H_n\}_{n \geqslant 0}$ est une famille génératrice. Indication : montrer que pour tout $P \in M$ de degré n, il existe $\lambda_0, \ldots, \lambda_n$ réels tels que $P = \sum_{k=0}^{n} \lambda_k H_k$, puis que $\lambda_k \in \mathbb{Z}$ pour tout k.

[1 pt] (a) Le polynôme nul est dans M et que la somme de deux polynômes de $\mathbb{R}[X]$ est dans M. Ainsi M est un sous-groupe de $\mathbb{R}[X]$, c'est en particulier un groupe commutatif i.e. un $\mathbb{Z}$-module.

[1 pt] (b) Soit $m \in \mathbb{Z}$. Si $m \geq n$, on a $H_n(m) = \binom{m}{n}$ qui est entier.

[1 pt] Si $0 \leq m \leq n-1$, on a $H_n(m) = 0$ et si $m < 0$, on a $H_n(m) = (1/n!)(m)(m-1)\ldots(m-n+1) = (1/n!)(-1)^n(-m)(-m+1)\ldots(-m+n-1) = (-1)^n\binom{-m+n-1}{n}$ qui est entier.

Dans tous les cas $H_n(m) \in \mathbb{Z}$, donc $H_n \in M$.

[2 pts] (c) Dans le $\mathbb{R}$-espace vectoriel $\mathbb{R}[X]$, la famille $\{H_n\}_{n \geqslant 0}$ est étagée par les degrés (i.e. à degrés tous distincts), donc c'est une famille libre. Ainsi toute combinaison linéaire finie des H_n à coefficients réels nulle a ses coefficients nuls ; ceci est vrai en particulier si les coefficients sont dans $\mathbb{Z}$, donc $\{H_n\}_{n \geqslant 0}$ est une famille libre du $\mathbb{Z}$-module M.

[2 pts] (d) Dans $\mathbb{R}_n[X] = \{Q \in \mathbb{R}[X], \deg(Q) \leq n\}$ la famille $\{H_k\}_{k \geqslant n}$ est libre et de cardinal $n+1$ donc c'est une $\mathbb{R}$-base. Ceci montre que pour tout $P \in M$ de degré n il existe $\lambda_0, \ldots, \lambda_n$ réels et uniques tels que $P = \sum_{k=0}^{n} \lambda_k H_k$. Montrons par récurrence sur $k \leq n$ que $\lambda_k \in \mathbb{Z}$. Pour $k = 0$ c'est vrai car $P(0) = \lambda_0$ qui est dans $\mathbb{Z}$ puisque $P \in M$. Pour $k \geq 1$ il suffit de calculer $P(k) = \lambda_0 + \lambda_1 H_1(k) + \cdots + \lambda_{k-1}H_{k-1}(k) + \lambda_k$, puisque $H_k(k) = 1$ et $H_k(\ell) = 0$ si $\ell > k$. Ainsi $\lambda_k = P(k) - \lambda_0 - \lambda_1 H_1(k) - \cdots - \lambda_{k-1}H_{k-1}(k) \in \mathbb{Z}$.