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

Feuille d'exercices 8 : indications de solutions

Exercice 1 - Non. La partie 2-primaire de A est isomorphe à $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$, celle de B à $\mathbb{Z}/8\mathbb{Z}$. On voit par exemple que B admet un élément d'ordre 8 mais que A n'en a pas. Si l'on calcule les facteurs invariants, on trouve $(18, 180)$ pour A et $(3, 1080)$ pour B.

Exercice 2 - Le théorème de structure implique que A contient un sous-groupe isomorphe à $(\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z})$, où $2 \leq d_1 \mid d_2$. Ce cernier contient les deux sous-groupes $(\mathbb{Z}/d_1\mathbb{Z}) \times \{0\}$ et $\{0\} \times (\frac{d_2}{d_1}\mathbb{Z}/d_2\mathbb{Z})$, qui sont distincts et cycliques d'ordre d_1.

Exercice 3 - 1 : posons $H := \{z \in K^* | z^d = 1\}$. Comme l'ordre de tout élément de G divise d, on a $G \subset H$. Mais d'autre aprt, H est l'ensemble des racines dans K du polynôme $X^d - 1$, donc $\operatorname{Card} H \leq d = \operatorname{Card} G$, d'où l'égalité. **2** : la question **1** montre que K^* admet au plus un sous-groupe fini d'ordre donné. La même propriété vaut donc pour tout sous-groupe fini de K^*, et l'exercice **2** permet d'en déduire qu'un tel sous-groupe est cyclique.

Exercice 5 - (i) un seul morphisme, le morphisme nul ; (ii) aucun sauf si A est nulle ; (iii) un seul morphisme, le morphisme structural.

Exercice 6 - 1 : pour l'injectivité, remarquer que $\mathrm{mul}_{\alpha,A}(1) = \alpha$. **2** : il résulte de **1** que α et mul_α ont les mêmes polynômes annulateurs. **3** : si A est de dimension finie n sur k, alors $\mathrm{End}_{k\text{-module}}(A)$ est isomorphe à $\mathrm{M}_n(k)$. **4** : l'application $\alpha \mapsto \mathrm{mul}_\alpha$ est un *anti-homomorphisme* de k-algèbres (elle « renverse la multiplication »).

Exercice 7 - 2 : remarquer que si $P = a_m X^m +$ (termes de degré $< m$) et si $Q = b_n X^n +$ (termes de degré $< n$), alors $PQ = a_m b_n X^{m+n} +$ (termes de degré $< m + n$). Si a_m est régulier et $b_n \neq 0$, alors $a_m b_n \neq 0$, donc $PQ \neq 0$. **3** : « seulement si » est trivial puisque k est un sous-anneau de $k[X]$, et « si » résulte de **2**. **6** : utiliser **1** et **3**. **7** : si P est nilpotent, alors $P(0)$ (le terme constant) l'est aussi donc $P - P(0)$ est nilpotent. Ce dernier est de la forme XQ avec $\deg Q < \deg P$, et Q est nilpotent (puisque X est régulier dans $k[X]$). On gagne donc par récurrence sur le degré. **8** : pour « si », utiliser **7**. **9** : un polynôme de la forme indiquée est somme d'un inversible et d'un nilpotent donc est inversible. Réciproquement, supposons $P = \sum_{i=0}^n a_i X^i$ inversible. Alors $a_0 = P(0)$ est inversible dans k. Montrons que a_j est nilpotent pour tout $j \geq 1$: il suffit pour cela de voir que les a_j appartiennent à tout idéal premier J de k. Or l'image de P par le morphisme canonique $k[X] \to k[X]/Jk[X] \cong (k/J)[X]$ est encore inversible, donc est constante puisque k/J est intègre (question **3**). Autrement dit les a_j $(j \geq 1)$ appartiennent à J, cqfd.

Exercice 13 - (i) vrai ; (ii) faux (prendre $\beta = -\alpha$) ; (iii) vrai (par l'absurde, en écrivant $\beta = (\alpha + \beta) - \beta$) ; (iv) vrai (si α est annulé par $\sum_{i=0}^d a_i X^i$, alors α^{-1} est annulé par $\sum_{i=0}^d a_i X^{d-i}$). (v) faux (prendre $\alpha = 0$) ; (vi) vrai ($\beta = \alpha^{-1}(\alpha\beta)$) ; (vii) vrai (si α est algébrique et régulier, il est inversible) ; (viii) vrai ; (ix) faux.

Exercice 14 - **1** : $\sqrt{2}+\sqrt{5}$ est racine de X^4-14X^2+9. **2** : x est racine de $X^6-9X^4-4X^3+27X^2-36X-23$.
3 : soit S l'ensemble des $\alpha^i\beta^j$ $(0 \leq i < m, 0 \leq j < n)$. Alors $\mathbb{Q}[\alpha,\beta]$ est engendré par S comme $\mathbb{Q}$ espace vectoriel. En particulier on peut écrire explicitement γ comme combinaison $\mathbb{Q}$-linéaire des éléments de S : par exemple on peut, par divisions euclidiennes successives par P et Q, écrire $F(X,Y) = A(X,Y)P(X) + B(X,Y)Q(Y) + R(X,Y)$ où R est de degré $< m$ en X et de degré $< n$ en Y ; on a alors $\gamma = R(\alpha,\beta)$. On peut aussi faire la même chose pour les puissances γ^k $(0 \leq k \leq mn)$. Il y en a $mn+1$, donc elles sont $\mathbb{Q}$-linéairement dépendantes puisque $\operatorname{Card} S \leq mn$. Par résolution d'un système linéaire à coefficients dans $\mathbb{Q}$, on peut trouver une relation de dépendance linéaire entre les γ^k, donc un polynôme de degré $\leq mn$ annulant γ.
Le même raisonnement peut se présenter de façon matricielle : $\mathbb{Q}(\alpha,\beta)$ est un quotient de la $\mathbb{Q}$-algèbre $A := \mathbb{Q}[X,Y]/(F(X),G(Y))$ qui admet pour base la famille des x^iy^j $(0 \leq i < m, 0 \leq j < n)$, où x et y sont les classes de X et Y. La matrice de la multiplication par x (resp. y) dans cette base se déduit directement de P (resp. Q) ; on peut donc en déduire la matrice Γ de la multiplication par $F(x,y)$ (élément de A dont l'image dans $\mathbb{Q}(\alpha,\beta)$ est γ). On est donc ramené au problème de trouver un polynôme annulateur d'une matrice carrée donnée, qui se résout par un système linéaire (ou, plus brutalement, par Cayley-Hamilton).

Exercice 15 - **1** : (i) $\mathrm{N}_{A/k}(\alpha) = 1$; (ii) $\mathrm{N}_{A/k}(\alpha) = \alpha^n$; (iii) $\mathrm{N}_{A/k}(\alpha_1,\ldots,\alpha_n) = \prod_{i=1}^n \alpha_i$; (iv) $\mathrm{N}_{A/k}(x+iy) = x^2+y^2$ $(x,y \in \mathbb{R})$; (v) $\mathrm{N}_{A/k}(x+y\sqrt{2}) = x^2-2y^2$ $(x,y \in \mathbb{Q})$; (vi) $\mathrm{N}_{A/k}(\alpha) = \det(\alpha)^p$. **2** : $\mathrm{N}_{A/k}(\alpha\beta) = \mathrm{N}_{A/k}(\alpha)\,\mathrm{N}_{A/k}(\beta)$. **3** : $\alpha \in A^\times$ si et seulement si mul_α est inversible. **4** : le seul changement consiste à remplacer, dans la question **3**, « $\mathrm{N}_{A/k}(\alpha) \neq 0$ » par « $\mathrm{N}_{A/k}(\alpha) \in k^\times$ ».

Exercice 16 - **3** : la liste des invariants de similitude est $(\mu_x,\ldots,\mu_x)$ (r fois) ; le polynôme caractéristique est $(-1)^d\mu_x^r$. **4** : $\mathrm{N}_{L/k}(x) = (-1)^d\mu_x(0)^r$. **5** : soit $(y_1,\ldots,y_r)$ une $K(x)$-base de L : prendre la concaténation des r familles $\left(y_j, xy_j, x^2y_j, \ldots, x^{\frac{d}{r}-1}y_j\right)$ $(1 \leq j \leq r)$.