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

Feuille d'exercices 9 : indications de solutions

Exercice 1 - **1** : $\omega(\omega^4-1)=1$ donc ω est inversible et $\omega^{-1}=\omega^4-1$. **2** : $\omega^{13}=2\omega^4+\omega^3+\omega+1$.

Exercice 2 - **1** : en bijection avec l'ensemble des éléments de A de carré nul.
3 et **4** : $(1,\varepsilon)$ est une base du $k[X]$-module $D_{k[X]}$, et $\partial(P)$ est la deuxième coordonnée de $P(X+\varepsilon)$ dans cette base. La formule pour $\partial(PQ)$ résultent de la formule de multiplication dans $D_{k[X]}$. **5** : on déduit de **4** que $\partial(1)=0$ et $\partial(X^n)=nX^{n-1}$ $(n\geq 1)$. Donc la dérivation et l'application ∂ coïncident sur la k-base $(X^n)_{n\in\mathbb{N}}$ de $k[X]$. Commes elles sont toutes deux k-linéaires, elles sont égales.

Exercice 3 - **1** : 1 pour $\mathbb{Q}$, 3 pour $\mathbb{R}$, 5 pour $\mathbb{C}$. **2** : pour tout élément e de carré nul dans une $\mathbb{Q}$-algèbre B, l'élément $x:=1+e$ vérifie $(x-1)^2=0$ donc $P(x)=0$, d'où un unique morphisme de A dans B envoyant la classe de X sur x. Pour $B=L$ il y a une infinité d'éléments de carré nul, à savoir les $\lambda\tau$ ($\lambda\in\mathbb{Q}$, $\tau=$ classe de T) donc une infinité de morphismes.

Exercice 4 - **1** : la matrice de mul_α dans la base $(1,\sqrt{d})$ est $\left(\begin{smallmatrix} x & dy \\ y & x\end{smallmatrix}\right)$; la norme est donc x^2-dy^2, la trace $2x$, et $\chi_\alpha(X)=X^2-2xX+x^2-dy^2$. **2** : en caractéristique 2, les formules sont vraies mais σ est l'identité. **3** : (notations précédentes) $\alpha^2\in K$ si et seulement si $\alpha\in K\cup K\sqrt{d}$; $u\in K$ est un carré dans L si et seulement si u ou u/d est un carré dans K.

Exercice 5 - **1** : si $\alpha':=\sqrt{2}-\sqrt{3}$ on a $\alpha\alpha'=-1$ donc $\alpha'\in K(\alpha)$, et par suite $\sqrt{2}=\frac{1}{2}(\alpha+\alpha')\in K(\alpha)$. Pour voir que $\alpha\notin\mathbb{Q}(\sqrt{2})$ on peut utiliser la question **3** de l'exercice **4** qui montre que $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$. On a $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$. **2** et **3** : on trouve que le polynôme $P:=X^4-10X^2+1$ annule α. Comme α est de degré 4 sur $\mathbb{Q}$ d'après **2**, P est le polynôme minimal de α sur $\mathbb{Q}$, et est donc irréductible.

Exercice 6 - Pour α : $X^6-6X^4-14X^3+12X^2-84X+41$. Pour β : $X^4+2X^3+5X^2+4X+1$. Pour γ : $X^4+2X^3-3X^2-4X+13$. Pour δ : X^4+2X^2+4. Pour ε : X^4-2X^2+9.

Exercice 7 - **1** : on a $[L(\alpha):L]=\deg Q$ donc $[L(\alpha):K]=m\deg Q\leq md$. Dautre part $K(\alpha)$ est un sous-corps de $L(\alpha)$ et est de degré d sur K. Donc $[L(\alpha):K]$ est multiple de m et de d, donc de md, d'où $[L(\alpha):K]=md$; ceci implique aussi que $\deg Q=d$ donc P est irréductible sur L.
2 : pour montrer l'irréductibilité de X^4+1, deux méthodes :
(1) s'il était réductible il serait de la forme $A(X)B(X)$ avec A et B unitaires irréductibles sur $\mathbb{Q}$ (il n'a pas de racine dans $\mathbb{Q}$). Mais la seule décomposition ce cette forme sur $\mathbb{R}$ est celle trouvée par le calcul, où A et B ne sont pas dans $\mathbb{Q}[X]$.
(2) Le changement de variable $X=Y+1$ donne $X^4+1=Y^4+6Y^3+4Y^2+6Y+2$ qui est irréductible par le critère d'Eisenstein.

Exercice 8 - **1** : $d\leq m$. **2** : on a $\mathrm{N}_{L/K}(a)=a^d$ puisque $a\in K$, et $\mathrm{N}_{L/K}(a)=\mathrm{N}_{L/K}(\alpha^m)=\mathrm{N}_{L/K}(\alpha)^m$; on peut donc prendre $b=\mathrm{N}_{L/K}(\alpha)$. **3** : si $ud+vm=1$, avec u et v entiers, on a

$a = a^{ud+vm} = (b^u\, a^v)^m$. **4** : si P n'a pas de racine alors $d > 1$ et d n'est pas premier avec m d'après **3**. Donc $d = m$. **5** : utiliser la décomposition de a en facteurs premiers pour voir que $a^d = b^m$ implique que m divise d, donc que $d = m$. (Remarque : pour cette question on peut aussi appliquer le critère d'Eisenstein, avec n'importe quel facteur premier de a).

Exercice 9 - 1 : remarquer que le membre de droite divise le membre de gauche, d'après le « petit théorème de Fermat ». **2** : le noyau est $\mathbb{F}_p$, d'après **1**. **3** ; l'ensemble des racines est $\alpha + \mathbb{F}_p$, et $P = \prod_{a\in\mathbb{F}_p}(X - \alpha - a)$. **4** : soit Q un facteur irréductible unitaire de P. Alors $Q = \prod_{a\in S}(X-\alpha-a)$ où S est une partie de $\mathbb{F}_p$, de cardinal s vérifiant $2 \leq s \leq p$. Le coefficient sous-dominant de Q est $-\sum_{a\in S}(\alpha + a) = -s\alpha + c$ avec $c \in K$. Donc $s\alpha \in K$; comme $\alpha \notin K$ on a donc $s1_K = 0$ donc p divise s et finalement $s = p$ et $Q = P$.
5 : si $X^p - X - a$ est réductible dans $\mathbb{Q}[X]$, il l'est dans $\mathbb{Z}[X]$ et est de la forme $A(X)B(X)$ avec A et B unitaires, à coefficients entiers, et non constants (réductibilité des polynômes sur un anneau factoriel). En particulier le polynôme est réductible modulo p, et a donc une racine dans $\mathbb{F}_p$ (question **4**). La classe de a modulo p est donc de la forme $x^p - x$ donc est nulle. (question **1**). Il suffit donc de choisir a non divisible par p.