Université Rennes 1, Année 2012-2013, Master 1 Math ALGB : Algèbre générale de base

Examen de deuxième session

Juin 2013

Seuls les résultats du cours pourront être admis. Documents et calculatrices ne sont pas autorisés.
Le barème envisagé, indiqué entre parenthèses, est donné à titre indicatif.

Justifiez toutes vos réponses !

Exercice 1 (6 points) Soit $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et $\alpha = \sqrt{2} + \sqrt{3} \in K$.

1. (2 points) Montrer que $[K : \mathbb{Q}] = 4$.
2. (1 point) L'extension $K/\mathbb{Q}$ est-elle galoisienne ? Si oui déterminer le groupe de Galois de l'extension $K/\mathbb{Q}$.
3. (2 points) Montrer que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ et déterminer le polynôme minimal $f_{\alpha,\mathbb{Q}}$ de α sur $\mathbb{Q}$.
4. (1 point) Déterminer le polynôme minimal $f_{\alpha,\mathbb{Q}(\sqrt{3})}$ de α sur $\mathbb{Q}(\sqrt{3})$.

Exercice 2 (4 points) Soient $f = X^3 + X + 1 \in \mathbb{F}_5[X]$, $K = \mathbb{F}_5[X]/(f)$ et $\alpha = \overline{X}$ l'image de X par le morphisme canonique $\pi : \mathbb{F}_5[X] \to \mathbb{F}_5[X]/(f)$.

1. (1 point) Montrer que K est un corps, donner sa caractéristique et son cardinal.
2. (2 points) Écrire α^3, α^{15} et α^{30} dans la $\mathbb{F}_5$-base $\mathcal{B} = (1, \alpha, \alpha^2)$ et en déduire l'ordre de α et de 2α dans le groupe multiplicatif K^*.
   Indication: vous devez trouver $\alpha^{30} = \alpha^2 + 1$. *Noter aussi que* $124 = 2^2 \cdot 31$.
3. (1 point) Donner le groupe de Galois de l'extension $K/\mathbb{F}_5$ et en déduire les zéros du polynôme minimal de $\beta = -\alpha - 1$ sur $\mathbb{F}_5$ dans une représentation de votre choix (pas forcément la base $\mathcal{B}$).

Exercice 3 (7 points) Soient A un anneau principal et a, b deux éléments non nuls de A. On note d (resp. m) un pgcd (resp. un ppcm) de a et b. On se propose de démontrer que la suite des facteurs invariants du A-module $M = A/(a) \oplus A/(b)$ est la suite (d, m).

1. (1 point) Énoncez le théorème de structure des A-modules de type fini.

   On rappelle que d et m sont définis à un inversible près et qu'on peut les choisir de telle sorte que $ab = dm$, ce que l'on supposera.

2. (2 points) Justifiez qu'il existe dans A des éléments a', b', u, v tels que $a = da'$, $b = db'$, $m = da'b'$ et $ua' + vb' = 1$.

3. (2 points) Justifiez avec soin que l'expression $\varphi(x, y) = (ux + vy, b'x - a'y)$ définit un morphisme de A-modules $\varphi : A/(a) \oplus A/(b) \to A/(d) \oplus A/(m)$.

4. (1 point) Justifiez avec soin que l'expression $\psi(s, t) = (a's + vt, b's - ut)$ définit un morphisme de A-modules $\psi : A/(d) \oplus A/(m) \to A/(a) \oplus A/(b)$.

5. (1 point) Montrez que φ et ψ sont des isomorphismes inverses l'un de l'autre et concluez.

Exercice 4 (3 points) Soient k un corps et $A = k[X]$ l'anneau des polynômes en une indéterminée à coefficients dans k. Soit $f : A \to A$ un endomorphisme de k-algèbres (c'est-à-dire un morphisme d'anneaux k-linéaire) et $Q = f(X)$ l'image du polynôme X par f.

1. (1 point) Montrez que pour tout $P \in A$ on a $f(P) = P(Q(X))$, de sorte que f est entièrement déterminé par $Q = f(X)$.

2. (2 points) Montrez que si f est un automorphisme alors $\deg(Q) = 1$, en observant que $\deg(P \circ Q) = \deg(P) \deg(Q)$. Réciproquement montrez que si $\deg(Q) = 1$, alors f est un automorphisme, en donnant explicitement son inverse.

Corrigé de l'exercice 1.

1. $X^2-3 \in \mathbb{Q}[X]$ étant irréductible (Eisensein dans $\mathbb{Z}[X]$ avec le premier $3 \in \mathbb{Z}$) et de zéro $\sqrt{3}$, c'est le polynôme minimal de $\sqrt{3}$ sur $\mathbb{Q}$. Donc $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ et

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3})(\sqrt{2}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \geqslant 2.$$

   $X^2 - 2 \in \mathbb{Q}[X] \subset \mathbb{Q}(\sqrt{3})[X]$ est divisible par le polynôme minimal $f_{\sqrt{2},\mathbb{Q}(\sqrt{3})} \in \mathbb{Q}(\sqrt{3})[X]$ de $\sqrt{2}$ sur $\mathbb{Q}(\sqrt{3})$ qui est donc de degré 1 ou 2. Supposons $f_{\sqrt{2},\mathbb{Q}(\sqrt{3})} \in \mathbb{Q}(\sqrt{3})[X]$ de degré 1. Alors $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$ et dans la $\mathbb{Q}$-base $(1, \sqrt{3})$ de l'extension $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ on a $\sqrt{2} = a_0 + a_1\sqrt{3}$ avec $a_i \in \mathbb{Q}$. Nous obtenons $2 = (a_0 + a_1\sqrt{3})^2 = a_0^2 + 2a_0a_1\sqrt{3} + 3a_1^2$ et il en résulte que $\sqrt{3} \in \mathbb{Q}$ qui contredit ce qui précède. Donc $[K : \mathbb{Q}] = 2 \cdot 2 = 4$.

2. $K = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3})$ est un corps de décomposition de $g = (X^2-2)(X^2-3) \in \mathbb{Q}[X]$. Comme $\mathbb{Q}$ est de caractéristique zéro l'extension $K/\mathbb{Q}$ est galoisienne et son groupe de Galois G est d'ordre $[K : \mathbb{Q}] = 4$ (il est donc isomorphe soit à $\mathbb{Z}/4\mathbb{Z}$ soit à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$). Un automorphisme $\sigma \in G$ est uniquement déterminé par son action sur les racines de g et envoie une racine d'un facteur de g sur une racine de ce même facteur. Donc $\sigma(\sqrt{2}) = \pm\sqrt{2}$ et $\sigma(\sqrt{3}) = \pm\sqrt{3}$ (l'image de $-\sqrt{2}$ et de $-\sqrt{3}$ en découle), ce qui livre quatre possibilités qui, puisque G est d'ordre 4, correspondent toutes à un automorphisme de $K/\mathbb{Q}$. Les automorphismes étant tous d'ordre deux il en résulte que $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3. Comme $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{3}, \sqrt{2})$ nous obtenons $4 = [K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$ qui montre que $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divise 4. Considérons la $\mathbb{Q}$-base de $K/\mathbb{Q}$ donnée par $\mathcal{B} = (1, \sqrt{3}, \sqrt{2}, \sqrt{3}\sqrt{2} = \sqrt{6})$. L'écriture $\alpha = \sqrt{3} + \sqrt{2}$ dans cette base étant unique nous obtenons $\alpha \notin \mathbb{Q}$. Supposons $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$, alors

$$0 = \alpha^2 + a_1\alpha + a_0 = (5 + a_0) + a_1\sqrt{3} + a_1\sqrt{2} + 2\sqrt{6} = 0$$

   avec $a_i \in \mathbb{Q}$ qui contredit le fait que $\mathcal{B}$ est une $\mathbb{Q}$-base. Donc $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Pour obtenir le polynôme minimal on note que $(\alpha - \sqrt{2})^2 = \alpha^2 - 2\alpha\sqrt{2} + 2 = 3$ et donc $(\alpha^2 - 1)^2 = 8\alpha$ qui montre que $X^2 - 10X + 1 \in \mathbb{Q}[X]$ est un polynôme annulateur de α de degré minimal sur $\mathbb{Q}$.

4. $[K : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ il en résulte que $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] = 2$. Comme $(\alpha - \sqrt{3})^2 = 2$ le polynôme $X^2 - 2\sqrt{3}X + 1 \in \mathbb{Q}(\sqrt{3})[X]$ est un polynôme annulateur de α de degré minimal sur $\mathbb{Q}(\sqrt{3})$.

Corrigé de l'exercice 2.

1. Le polynôme f étant de degré 3 et n'admettant pas de zéro dans $\mathbb{F}_5$ est irréductible (par exemple $4^3 + 4 + 1 = 69$ n'est pas divisible par 5). Comme $\mathcal{B} = (1, \alpha, \alpha^2)$ est une $\mathbb{F}_5$-base de K, il existe 5^3 éléments dans K. Le corps premier de K étant $\mathbb{F}_5$ il est de caractéristique 5.

2. Dans K on calcule modulo X^3+X+1 et $\alpha^3 = -\alpha - 1$. D'où $\alpha^4 = -\alpha^2 - \alpha$, $\alpha^5 = -\alpha^3 - \alpha^2 = -\alpha^2 + \alpha + 1$, $(\alpha^3)^5 = (-\alpha-1)^5 = -\alpha^5 - 1 = \alpha^2 - \alpha + 3$ et $\alpha^{30} = (\alpha^2 - \alpha + 3)^2 = \alpha^2 + 1$. Le groupe multiplicatif K^* est d'ordre $125 - 1 = 2^2 \cdot 31$ et l'ordre de α doit diviser ce nombre. L'écriture dans la base $\mathcal{B}$ étant unique l'ordre de α n'est ni $2, 4$ et $\alpha^{31} = \alpha^{30}\alpha = -1$. Comme $\alpha^{62} = (\alpha^2+1)^2 = 1$ l'ordre de α est 62. Pour calculer $(2\alpha)^2, (2\alpha)^4, (2\alpha)^{31}$ et , $(2\alpha)^{62}$ on multiplie les expressions précédentes dans la base $\mathcal{B}$ par $2^2 = -1, 2^4 = 2, 2^{31} = 2, 2^{62} = 2^2$ en utilisant $2^5 = 2$. Ainsi 2α est d'ordre 124 et est donc un générateur de K^*.

3. D'après le cours le groupe de Galois est cyclique d'ordre $3 = [K : \mathbb{F}_5]$ et est engendré par le morphisme de Frobénius $z \mapsto z^5$. Puisque $\mathbb{F}_5(\alpha^3) \subset K$ le degré $[\mathbb{F}_5(\alpha^3) : \mathbb{F}_5]$ divise $[K : \mathbb{F}_5] = 3$. Comme $-1 - \alpha = \alpha^3$ n'appartient pas à $\mathbb{F}_5$ le polynôme minimal $g \in \mathbb{F}_5[X]$ de α^3 est d'ordre 3. Le groupe de Galois envoie une racine de g sur une racine de g et donc $(\alpha^3)^5$ et $((\alpha^3)^5)^5$ sont les deux autres racines de g.

Corrigé de l'exercice 3.

1. Soit M un A-module de type fini. Alors il existe un entier $n \geqslant 0$ et des éléments $d_1, \ldots, d_r$ de A, non inversibles et éventuellement nuls, tels que $d_1 \mid \cdots \mid d_r$ et :

$$M \simeq A/(d_1) \oplus \cdots \oplus A/(d_n).$$

2. Comme d est un diviseur commun de a et b, il existe des éléments a', b' tels que $a = da'$ et $b = db'$. Comme de plus d est un *plus grand* diviseur commun, nécessairement a' et b' sont premiers entre eux. D'après le théorème de Bézout, il existe alors $u, v \in A$ tels que $ua' + vb' = 1$. Enfin, comme $ab = md$, on obtient $m = da'b'$.

3. Il est clair que les expressions $ux + vy$ et $b'x - a'y$ sont A-linéaires en x et y, donc on peut définir un morphisme de A-modules $\varphi_1 : A \oplus A \to A \oplus A$ par $\varphi_1(x, y) = (ux + vy, b'x - a'y)$. Notons $\varphi_2 : A \oplus A \to A/(d) \oplus A/(m)$ le morphisme composé de φ_1 avec les morphismes de quotient $A \to A/(d)$ et $A \to A/(m)$. Maintenant, si $x \in (a)$ et $y \in (b)$, il existe x', y' tels que $x = ax'$ et $y = by'$, donc

$$\begin{aligned}\varphi_2(x, y) &= (ux + vy, b'x - a'y) \\ &= (uax' + vby', b'ax' - a'by') \\ &= (d(ua'x' + vb'y'), m(x' - y')) \\ &= 0\end{aligned}$$

puisque la classe de d est nulle dans $A/(d)$ et celle de m nulle dans $A/(m)$. Ainsi $(a) \oplus (b) \subset \ker(\varphi_2)$ et il s'ensuit que φ_2 passe au quotient en un morphisme $\varphi : A/(a) \oplus A/(b) \to A/(d) \oplus A/(m)$ comme demandé.

4. Les mêmes arguments que dans la question précédente montrent que l'on peut définir un morphisme de A-modules $\psi_2 : A \oplus A \to A/(a) \oplus A/(b)$ par $\psi_2(s, t) = (a's + vt, b's - ut)$.

Si $s \in (d)$ et $t \in (m)$, il existe s', t' tels que $s = ds'$ et $t = mt'$, donc

$$\begin{aligned}\psi_2(s,t) &= (a's + vt, b's - ut)\\ &= (as' + mvt', bs' - mut')\\ &= (a(s' + b'vt'), b(s' - a'ut'))\\ &= 0\end{aligned}$$

puisque la classe de a est nulle dans $A/(a)$ et celle de b nulle dans $A/(b)$. Ainsi $(d) \oplus (m) \subset \ker(\psi_2)$ et il s'ensuit que ψ_2 passe au quotient en un morphisme $\psi : A/(d) \oplus A/(m) \to A/(a) \oplus A/(b)$ comme demandé.

5. On a :

$$\begin{aligned}\psi(\varphi(x,y)) &= \psi(ux + vy, b'x - a'y)\\ &= (a'(ux + vy) + v(b'x - a'y), b'(ux + vy) - u(b'x - a'y))\\ &= (x,y)\end{aligned}$$

et

$$\begin{aligned}\varphi(\psi(s,t)) &= \varphi(a's + vt, b's - ut)\\ &= (u(a's + vt) + v(b's - ut), b'(a's + vt) - a'(b's - ut))\\ &= (s,t).\end{aligned}$$

Ceci montre que φ et ψ sont des isomorphismes inverses l'un de l'autre. Ainsi le module $M = A/(a) \oplus A/(b)$ est isomorphe à $A/(d) \oplus A/(m)$, et comme d divise m, on reconnaît que (d, m) est la suite des facteurs invariants de M.

Corrigé de l'exercice 4.

1. Notons $d = \deg(P)$ et $P = \sum_{i=0}^{d} p_i X^i$. Comme f est un morphisme d'anneaux k-linéaire, on a

$$f(P) = f(\sum_{i=0}^{d} p_i X^i) = \sum_{i=0}^{d} p_i f(X^i) = \sum_{i=0}^{d} p_i (f(X))^i = \sum_{i=0}^{d} p_i Q^i = P(Q(X)).$$

2. Si f est un automorphisme, en particulier il est surjectif, donc il existe P tel que $f(P) = P(Q(X)) = X$. Comme $\deg(P \circ Q) = \deg(P)\deg(Q)$, on en déduit en prenant les degrés que $\deg(P)\deg(Q) = 1$. Il s'ensuit que $\deg(P) = \deg(Q) = 1$. Réciproquement, si $\deg(Q) = 1$ on peut écrire $Q = aX + b$ avec $a \in k^\times$ et $b \in k$. Posons $Q' = a^{-1}(X - b)$ et soit $f' : A \to A$ l'endomorphisme déterminé par $f'(X) = Q'$, qui est donc tel que $f'(P) = P(Q'(X))$. On a $f(X) = aX + b$ puis $(f' \circ f)(X) = f(aX + b) = a^{-1}(aX + b - b) = X$, donc $f' \circ f$ est l'identité de A. De même on a $f'(X) = a^{-1}(X - b)$ puis $(f \circ f')(X) = f(a^{-1}X - a^{-1}b) = a(a^{-1}X - a^{-1}b) + b = X$, donc $f \circ f'$ est l'identité de A. Finalement f' est un inverse pour f, donc f est un automorphisme.