

Avertissement : Pour obtenir une très bonne note, il n'est pas nécessaire de répondre à l'ensemble des questions.

1. Déterminer le groupe de Galois sur $\mathbb{Q}$ des polynômes suivants :

(a) $t^8 + 1$;

(b) $32t^5 + 16t^4 - 32t^3 - 12t^2 + 6t + 1 = 32 \prod_{i=1}^5 (t - \cos(\frac{2i\pi}{11}))$;

(c) $t^5 - 70t^4 - 49t^3 - 70t^2 + 98t + 105$.

Corrigé. (a) Le corps de décomposition sur $\mathbb{Q}$ de $t^8 + 1$ est $\mathbb{Q}(\zeta)$ avec ζ une racine primitive 16-ième de l'unité (les racines primitives 16-ièmes, $\zeta, \zeta^3, \zeta^5, \dots, \zeta^{15}$ sont même exactement les racines de $t^8 + 1$) : donc le groupe de Galois est $(\mathbb{Z}/16\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$.

(b) Soit $E = \mathbb{Q}(\zeta)$ où ζ est une racine primitive 11-ième de l'unité : ainsi, $\text{Gal}(E/\mathbb{Q}) = (\mathbb{Z}/11\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$. En appelant L le corps de décomposition du polynôme considéré, c'est-à-dire engendré par les $\cos(\frac{2i\pi}{11}) = \frac{1}{2}(\zeta^i + \zeta^{-i})$, on a manifestement $\mathbb{Q} \subseteq L \subseteq E$, donc $\text{Gal}(L/\mathbb{Q})$ est le quotient de $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ par $\text{Gal}(E/L)$; or ce dernier contient la conjugaison complexe, qui est d'ordre 2, et ζ vérifie sur L l'équation $\zeta^2 - 2\cos(\frac{2\pi}{11})\zeta + 1 = 0$, bref $[E : L] = 2$ et $[L : \mathbb{Q}] = 5$ et on peut conclure $\text{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$.

(c) La réduction modulo 2 de ce polynôme est $t^5 + t^3 + 1$, qui est irréductible (pour s'en convaincre, il suffit par exemple de constater que modulo $t^5 + t^3 + 1$ on a $t^{32} \equiv t$, ce qui peut se faire en élevant successivement au carré : $t^8 \equiv t^4 + t^3 + t$ donc $t^{16} \equiv t^3 + t^2$ et $t^{32} \equiv t$). Quant à la réduction modulo 5, elle se factorise comme $t^5 + t^3 - 2t = t(t+1)(t-1)(t^2+2)$ et le facteur $t^2 + 2$ est irréductible : de ces deux considérations on déduit qu'il y a dans le groupe de Galois sur $\mathbb{Q}$, agissant sur les cinq racines, une transposition et un 5-cycle, or il est facile de voir qu'une transposition et un 5-cycle engendrent toujours $\mathfrak{S}_5$ (on peut supposer que le 5-cycle est $(1\ 2\ 3\ 4\ 5)$ et que la transposition est $(1\ x)$ avec x valant 2 ou 3). Le groupe de Galois est donc $\mathfrak{S}_5$.

On pouvait aussi remarquer que le polynôme est d'Eisenstein en 7 pour obtenir l'irréductibilité : avec la réduction modulo 5 cela permet de conclure car tout sous-groupe transitif de $\mathfrak{S}_5$ contenant une transposition est tout $\mathfrak{S}_5$. La transposition pouvait aussi s'obtenir en constatant que le polynôme a deux racines complexes conjuguées (mais c'est beaucoup plus fastidieux que de réduire modulo 5). On pouvait aussi déduire de la réduction modulo 3, à savoir $t^5 - t^4 - t^3 - t^2 - t = t(t-1)(t^3 - t + 1)$ l'existence d'un 3-cycle dans le groupe de Galois (mais ça n'exclut pas la possibilité de $\mathfrak{A}_5$). ✓

2. Soient $n \geq 1$ un entier et R un anneau commutatif. Soient L le module libre R^{2n} et A une matrice de format $2n \times 2n$ à coefficients dans R qui est antisymétrique, c'est-à-dire que l'on a $a_{ii} = 0$ et $a_{ij} = -a_{ji}$ pour tous $1 \leq i, j \leq 2n$. On définit l'élément $\omega(A)$ de $\bigwedge^{2n}(L)$ par

$$\omega(A) = \sum_{i < j} a_{ij} e_i \wedge e_j$$

(a) Supposons que $n = 2$. Expliciter un polynôme Pf en les variables X_{ij} , $1 \leq i < j \leq 4$, à coefficients entiers tel qu'on ait

$$\omega(A)^2 = 2 \text{ Pf}(A) e_1 \wedge e_2 \wedge e_3 \wedge e_4$$

(b) Montrer qu'il existe un unique polynôme Pf, le *pfaffien*, à coefficients entiers en les variables X_{ij} , $1 \leq i < j \leq n$, tel qu'on ait

$$\omega(A)^n = n! \text{ Pf}(A) e_1 \wedge \dots \wedge e_{2n}$$

quels que soient R et A .

(c) Soit $f: R^{2n} \rightarrow R^{2n}$ une application R -linéaire de matrice B dans la base canonique. Montrer qu'on a

$$\omega(B A^t B) = \bigwedge^2(f) (\omega(A))$$

En déduire qu'on a

$$\text{Pf}(B A^t B) = \det(B) \text{Pf}(A)$$

quels que soient R , A et B .

(d) Supposons que R est un corps et que A est inversible. Rappelons qu'il existe alors une matrice inversible B telle que $A = B J^t B$, où

$$J = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}$$

Montrer que l'on a

$$\det(A) = \text{Pf}(A)^2$$

(e) Montrer que l'on a $\det = \text{Pf}^2$, pour une matrice antisymétrique, dans l'anneau des polynômes à coefficients entiers en les variables X_{ij} , $1 \leq i, j \leq 2n$.

Corrigé. (a) Pour $n = 4$, on a $\omega(A) = a_{12} e_1 \wedge e_2 + a_{13} e_1 \wedge e_3 + a_{14} e_1 \wedge e_4 + a_{23} e_2 \wedge e_3 + a_{24} e_2 \wedge e_4 + a_{34} e_3 \wedge e_4$. En développant $\omega(A)^2$, chacun de ces six termes n'a un produit non nul qu'avec un seul autre, et on trouve $\omega(A)^2 = 2(a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23}) e_1 \wedge e_2 \wedge e_3 \wedge e_4$, d'où le polynôme recherché, $X_{12}X_{34} - X_{13}X_{24} + X_{14}X_{23}$.

(b) En développant complètement $\omega(A)^2$, seuls subsistent les termes produits de $a_{ij} e_i \wedge e_j$ où tous les i et j qui interviennent dans les différents facteurs sont distincts. On peut donc écrire $\omega(A)^2 = \sum_{\gamma, \gamma'} \prod_{i=1}^n a_{\gamma(i)\gamma'(i)} e_{\gamma(i)} \wedge e_{\gamma'(i)}$ où la somme porte sur les couples (γ, γ') d'injections $\{1, \dots, n\} \rightarrow \{1, \dots, 2n\}$ à images disjointes et vérifiant $\gamma(i) < \gamma'(i)$ pour tout i (et le produit a un sens vu que sur les éléments de degré pair la multiplication dans $\bigwedge^{2n}(L)$ est commutative).

En réordonnant chaque produit pour faire intervenir $\vec{e} = e_1 \wedge \dots \wedge e_{2n}$, on voit que chaque $\prod_{i=1}^n a_{\gamma(i)\gamma'(i)} e_{\gamma(i)} \wedge e_{\gamma'(i)}$ se réécrit $\varepsilon(\gamma||\gamma') \left(\prod_{i=1}^n a_{\gamma(i)\gamma'(i)} \right) \vec{e}$, c'est-à-dire affublé d'un signe $\varepsilon(\gamma||\gamma')$ qui est le signe de la permutation $\gamma||\gamma'$ de $\{1, \dots, 2n\}$ obtenu en intercalant γ et γ' (formellement, pour $1 \leq i \leq n$, on a $(\gamma||\gamma')(2i-1) = \gamma(i)$ et $(\gamma||\gamma')(2i) = \gamma'(i)$).

Or, pour γ, γ' deux injections $\{1, \dots, n\} \rightarrow \{1, \dots, 2n\}$ à images disjointes, cette signature $\varepsilon(\gamma||\gamma')$ ne dépend que de l'ensemble des couples $(\gamma(i), \gamma'(i))$ (puisque, de nouveau, les $e_{\gamma(i)} \wedge e_{\gamma'(i)}$ commutent entre eux), et donc, avec la contrainte $\gamma(i) < \gamma'(i)$, de l'ensemble $\mathcal{B}$ des paires $\{\gamma(i), \gamma'(i)\}$.

On peut donc réécrire $\omega(A)^2$ comme, sur tous les couples (γ, γ') comme précédemment, des termes $\varepsilon(\mathcal{B}) \left(\prod_{b \in \mathcal{B}} a_b \right) \vec{e}$, avec $\mathcal{B} = \{\{\gamma(i), \gamma'(i)\}\}$, où $a_b = a_{ij}$ si $b = \{i, j\}$ avec $i < j$, et $\varepsilon(\mathcal{B}) = \varepsilon(\gamma||\gamma')$. Chaque partition $\mathcal{B}$ de $\{1, \dots, 2n\}$ en parties à deux éléments donne, dans cette somme, $n!$ termes tous égaux, un pour chaque γ (énumérant l'ensemble des min b pour $b \in \mathcal{B}$), γ' étant alors uniquement déterminé : on a ainsi $\omega(A)^2 = n! \sum_{\mathcal{B}} \varepsilon(\mathcal{B}) \left(\prod_{b \in \mathcal{B}} a_b \right) \vec{e}$, où $\mathcal{B}$ parcourt les partitions de $\{1, \dots, 2n\}$ en parties à deux éléments. On a donc défini $\text{Pf}(A) = \sum_{\mathcal{B}} \varepsilon(\mathcal{B}) \prod_{b \in \mathcal{B}} a_b$, qui est manifestement un polynôme universel à coefficients entiers en les $X_b = X_{ij}$ (si on veut, on applique ce qui précède à la matrice A sur $R = \mathbb{Z}[(X_{ij})_{i < j}]$ dont les coefficients sont les indéterminées, et on spécialise).

(c) Appelons a'_{ij} les coefficients de la matrice $B A^t B$ (manifestement antisymétrique), de sorte que $\omega(B A^t B) = \sum_{i < j} a'_{ij} e_i \wedge e_j$ où $a'_{ij} = \sum_{k, \ell} b_{ik} b_{j\ell} a_{k\ell}$. Mais on peut alors écrire $\sum_{i < j} a'_{ij} e_i \wedge e_j = \sum_{i < j} \sum_{k, \ell} b_{ik} b_{j\ell} a_{k\ell} e_i \wedge e_j = \sum_{i < j} \sum_{k < \ell} (b_{ik} b_{j\ell} - b_{i\ell} b_{jk}) a_{k\ell} e_i \wedge e_j$. Ceci vaut donc encore $\sum_{k < \ell} a_{k\ell} \sum_{i < j} (b_{ik} b_{j\ell} - b_{i\ell} b_{jk}) e_i \wedge e_j$. Mais $\sum_{i < j} (b_{ik} b_{j\ell} - b_{i\ell} b_{jk}) e_i \wedge e_j =$

$\sum_{i,j} b_{ik} b_{j\ell} e_i \wedge e_j = f(e_k) \wedge f(e_\ell)$. On a donc prouvé que $\omega(B A^t B) = \sum_{k < \ell} a_{k\ell} f(e_k) \wedge f(e_\ell) = \bigwedge^2(f) (\omega(A))$.

En particulier, $\omega(B A^t B)^n = \bigwedge^{2n}(f) (\omega(A)^n) = \det(B) \omega(A)^n$, ce qui donne exactement $\text{Pf}(B A^t B) = \det(B) \text{Pf}(A)$.

(d) La formule précédente appliquée à $A = B J^t B$ donne $\text{Pf}(A) = \det(B) \text{Pf}(J)$. Mais $\text{Pf}(J)$ est manifestement un signe (en l'occurrence $(-1)^{n(n-1)/2}$ mais peu importe) vu que, dans l'expression $\sum_{\mathcal{B}} \varepsilon(\mathcal{B}) \prod_{b \in \mathcal{B}} J_b$ obtenue plus haut, une seule partition $\mathcal{B}$ (à savoir $\{\{1, n+1\}, \{2, n+2\}, \dots, \{n, 2n\}\}$) donne un terme non nul : donc $\text{Pf}(A)^2 = \det(B)^2 = \det(A)$.

(e) Les polynômes $\det$ et Pf^2 (éléments de $\mathbb{Z}[(X_{ij})_{i < j}]$) prennent les mêmes valeurs sur un ouvert des matrices $A \in \mathbb{M}_{2n}(\mathbb{R})^{\text{antisym}}$, donc ils sont égaux. ✓

3. Soit A un anneau (commutatif ou non commutatif). Un A -module (à gauche) P est *projectif* s'il existe un A -module Q tel que $P \oplus Q$ est libre.

(a) Observer que tout module libre est projectif. Donner un exemple d'anneau A et de module P qui est projectif mais n'est pas libre.

(b) Montrer qu'on a équivalence entre

(i) P est projectif ;

(ii) pour tout morphisme surjectif de A -modules $f: M \rightarrow P$, il existe un morphisme $g: P \rightarrow M$ tel que $fg = \text{id}_P$.

(c) Montrer qu'un A -module P est projectif et de type fini ssi il existe un A -module Q tel que $P \oplus Q$ est libre de type fini.

(d) Supposons que A est un anneau commutatif et local, c'est-à-dire qu'il admet un unique idéal maximal. Notons $\mathfrak{m}$ cet idéal et k le corps $A/\mathfrak{m}$. Montrer que tout A -module projectif et de type fini est libre. Indication : on pourra construire une base de P en relevant une base de l'espace vectoriel $P/\mathfrak{m}P$.

Corrigé. (a) Si P est libre, P est projectif puisque $P \oplus 0$ est libre. La réciproque n'est pas vraie : $P = \mathbb{Z}/2\mathbb{Z}$ est un module projectif sur $A = \mathbb{Z}/6\mathbb{Z}$ puisque $A \oplus Q = A$ avec $Q = \mathbb{Z}/3\mathbb{Z}$, mais manifestement P n'est pas libre.

(b) Si $P \oplus Q$ est libre, et $f: M \rightarrow P$ est A -linéaire et surjective, considérons $f \oplus \text{id}_Q: M \oplus Q \rightarrow P \oplus Q$: visiblement elle est encore surjective. En relevant les éléments d'une base de $P \oplus Q$ on peut donc trouver $g_1: P \oplus Q \rightarrow M \oplus Q$ tel que $(f \oplus \text{id}_Q)g_1 = \text{id}_{P \oplus Q}$. Mais alors si $x \in P$ est vu comme $(x, 0) \in P \oplus Q$, on a $g_1(x, 0) = (y, z)$ vérifiant $f(y) = x$ et $z = 0$: donc en définissant g comme la composée $P \rightarrow P \oplus Q \xrightarrow{g_1} M \oplus Q \rightarrow M$, on a $y = g(x)$ qui vérifie $f(y) = x$, ce qu'on voulait : ceci démontre (ii).

Réciproquement, si P vérifie (ii), soit $f: A^{(I)} \rightarrow P$ une surjection (A -linéaire) quelconque vers P depuis un module libre (par exemple, on peut prendre pour I l'ensemble sous-jacent à P , ou en fait n'importe quelle partie génératrice, et f envoyant une combinaison A -linéaire formelle d'éléments de P sur la combinaison en question dans P), et soit $g: P \rightarrow A^{(I)}$ une section de f dont l'existence est garantie par (ii). Alors en posant $Q = \ker f$ et en identifiant P à $\text{im } g$, on a $P \oplus Q = A^{(I)}$.

(c) Si P est projectif de type fini, en reprenant la démonstration de (i) $\Rightarrow$ (ii) ci-dessus avec I fini, on voit qu'on peut écrire $P \oplus Q = A^I$ libre de type fini. Réciproquement, si $P \oplus Q$ est libre de type fini, manifestement P est projectif, mais il est aussi de type fini comme quotient de $P \oplus Q$ (image par la surjection canonique).

(d) Soit P un module projectif de type fini sur A (commutatif local). Considérons $\bar{P} = P/\mathfrak{m}P$, espace vectoriel sur $k = A/\mathfrak{m}$. Soit $\bar{e}_1, \dots, \bar{e}_r$ une base de $\bar{P}$ comme k -espace vectoriel (finie car P est de type fini) : d'après le lemme de Nakayama, si $e_1, \dots, e_r$ sont des

relèvements quelconques des $\bar{e}_i$ à P , alors ils engendrent P , c'est-à-dire que $f: A^r \rightarrow P$ (envoyant $(a_1, \dots, a_r)$ sur $a_1 e_1 + \dots + a_r e_r$) est surjective. Et d'après ce qu'on a déjà expliqué sur les modules projectifs, on peut écrire $A^r = P \oplus Q$ en identifiant P à l'image d'une injection $g: P \rightarrow A^r$ telle que $fg = \text{id}_P$ et Q au noyau de f . Pour conclure, il s'agit de prouver que $Q = 0$ (c'est-à-dire que f est un isomorphisme). Or si $x \in Q$ on a $a_1 \bar{e}_1 + \dots + a_r \bar{e}_r = 0 \in \bar{P}$ donc $a_i \in \mathfrak{m}$ pour tout i , c'est-à-dire que $Q \subseteq \mathfrak{m}^r$. Mais on a mieux : puisque $A^r = P \oplus Q$ donc aussi $\mathfrak{m}^r = \mathfrak{m}P \oplus \mathfrak{m}Q$, et que la projection d'un élément $x \in Q$ sur le premier terme dans cette décomposition est $f(x) = 0$, on a $Q = \mathfrak{m}Q$. Mais d'après le lemme de Nakayama (vu que Q , comme quotient de A^r est encore de type fini) ceci implique $Q = 0$, ce qu'il fallait démontrer. ✓

4. Soient K un corps et A une K -algèbre de dimension finie (non nécessairement commutative). L'algèbre A est *séparable* si l'application de multiplication $\mu: A \otimes_K A \rightarrow A$ admet une section σ qui est A -linéaire à gauche et à droite, c'est-à-dire que σ est une application K -linéaire de A dans $A \otimes_K A$ telle que $\mu\sigma = \text{id}_A$ et $a\sigma(b) = \sigma(ab) = \sigma(a)b$ pour tous a et b dans A .

(a) Montrer que A est séparable si et seulement si il existe un élément ρ dans $A \otimes_K A$ tel que $\mu(\rho) = 1$ et $a\rho = \rho a$ pour tous a dans A .

(b) Montrer que $M_n(K)$ est séparable pour tout entier $n \geq 1$. Indication : essayer $\rho = \sum_{i=1}^n E_{i1} \otimes E_{1i}$.

(c) Montrer qu'un produit de deux algèbres est séparable si et seulement si chacun des facteurs l'est.

(d) Montrer qu'une algèbre semi-simple de dimension finie sur un corps algébriquement clos est séparable.

(e) Supposons que A est séparable et que B est une K -algèbre quelconque. Soit

$$\rho = \sum_{i=1}^n a'_i \otimes a''_i$$

un élément comme dans (a). Soient M et M' des $A \otimes_K B$ -modules et $p: M \rightarrow M'$ un morphisme B -linéaire. Montrer que l'application $\bar{p}: M \rightarrow M'$ qui envoie un élément m de M sur

$$\sum_{i=1}^n a'_i p(a''_i m)$$

est $A \otimes_K B$ -linéaire. Montrer que si M' est un sous-module de M et que la restriction de p à M' est l'identité, alors la restriction de $\bar{p}$ à M' est l'identité.

(f) Montrer que si A est séparable et que B est une K -algèbre semi-simple, alors $A \otimes_K B$ est semi-simple.

(g) Montrer que A est semi-simple ssi A^{op} l'est. Indication : l'espace vectoriel DA des formes linéaires $f: A \rightarrow K$ devient un A -module pour l'action donnée par $(af)(b) = f(ba)$ et les sous-modules de DA sont en bijection naturelle avec les sous-modules du A^{op} -module libre A^{op} .

(h) Montrer que A est séparable si et seulement si $A \otimes_K B$ est semi-simple pour toute K -algèbre semi-simple B si et seulement si $A \otimes_K A^{\text{op}}$ est semi-simple.

Corrigé. (a) Si A est séparable, $\rho = \sigma(1)$ (où σ est une section (A, A) -linéaire de μ) vérifie $\mu(\rho) = 1$ et $a\rho = a\sigma(1) = \sigma(a) = \sigma(1)a = \rho a$ pour tout $a \in A$. Réciproquement, si un tel élément ρ existe, on définit $\sigma: A \rightarrow A \otimes_K A$ par $\sigma(a) = a\rho$: on a $\mu\sigma(a) = \mu(a\rho) = a$ pour tout a , et $a\sigma(b) = ab\rho = \sigma(ab) = a\rho b = \sigma(a)b$.

(b) Soit $\rho = \sum_{i=1}^n E_{i1} \otimes E_{1i} \in \mathbb{M}_n(K) \otimes_K \mathbb{M}_n(K)$, où E_{ij} est la base canonique de $\mathbb{M}_n(K)$. On a $\mu(\rho) = \sum_{i=1}^n E_{i1} E_{1i} = \sum_{i=1}^n E_{ii} = 1$, et si $a \in \mathbb{M}_n(K)$ est quelconque, qu'on décompose comme $a = \sum_{k,\ell} a_{k\ell} E_{k\ell}$, alors $a\rho = \sum_{i=1}^n a E_{i1} \otimes E_{1i} = \sum_{i,k,\ell} a_{k\ell} E_{k\ell} E_{i1} \otimes E_{1i} = \sum_{k,\ell} a_{k\ell} E_{k1} \otimes E_{1\ell}$ et de même $\rho a = \sum_{i=1}^n E_{i1} \otimes E_{1i} a = \sum_{k,\ell} E_{k1} \otimes E_{1\ell} a_{k,\ell}$ donc $a\rho = \rho a$.

(c) Soient A' et A'' deux K -algèbres de dimension finie, et $A = A' \times A''$ (comme K -espaces vectoriels, $A = A' \oplus A''$, et on a bien sûr $1_A = (1_{A'}, 1_{A''})$ qu'on pourra écrire $1_{A'} + 1_{A''}$ en identifiant A' et A'' à $A' \oplus 0$ et $0 \oplus A''$ respectivement).

Si A' et A'' sont séparables, soient ρ', ρ'' tels que donnés par la question (a) témoignant de la séparabilité de A' et A'' , et dans l'écriture $A \otimes_K A = (A' \otimes_K A') \oplus (A' \otimes_K A'') \oplus (A'' \otimes_K A') \oplus (A'' \otimes_K A'')$ considérons l'élément $\rho = \rho' + 0 + 0 + \rho''$. On a alors d'une part $\mu(\rho) = 1_{A'} + 1_{A''} = 1_A$ et d'autre part pour $a = (a', a'') \in A$ on a $a\rho = a'\rho' + 0 + 0 + a''\rho'' = \rho a$. Donc $A = A' \times A''$ est séparable.

Réciproquement, si A est séparable, considérons la décomposition de $\rho \in A \otimes_K A$ sur l'écriture $A \otimes_K A = (A' \otimes_K A') \oplus (A' \otimes_K A'') \oplus (A'' \otimes_K A') \oplus (A'' \otimes_K A'')$, mettons $\rho = \rho' + \delta_1 + \delta_2 + \rho''$. En observant $1_{A'}\rho = \rho' + \delta_1 + 0 + 0$ et $\rho 1_{A'} = \rho' + 0 + \delta_2 + 0$ on voit que $\delta_1 = \delta_2 = 0$: ainsi $\rho = \rho' + 0 + 0 + \rho''$ avec $\rho' \in A' \otimes_K A'$ et $\rho'' \in A'' \otimes_K A''$. On a $1_A = \mu(\rho) = \mu(\rho') + \mu(\rho'')$ donc $\mu(\rho') = 1_{A'}$ et $\mu(\rho'') = 1_{A''}$; enfin, si $a = (a', a'') \in A$, alors $a\rho = a'\rho' + 0 + 0 + a''\rho''$ donc $a\rho = \rho a$ implique $a'\rho' = \rho'a'$ et $a''\rho'' = \rho''a''$. Ceci prouve que A' et A'' sont séparables.

(d) On a vu aux questions précédentes que les algèbres de matrices sont séparables et que les produits d'algèbres séparables sont séparables : or si K est algébriquement clos, toute algèbre semi-simple de dimension finie sur K est un produit d'algèbre de matrices sur K — elle est donc séparable.

(e) Manifestement $\bar{p}$ est additif ($\mathbb{Z}$ -linéaire, et même K -linéaire). Si $b \in B$ et $m \in M$ alors $\bar{p}$ envoie bm (c'est-à-dire $(1_A \otimes b)m$) sur $\sum_i a'_i p(a''_i bm) = \sum_i a'_i b p(a''_i m) = b \bar{p}(m)$, donc la B -linéarité est claire (insistons sur le fait que, dans $A \otimes_K B$, les éléments provenant de A , c'est-à-dire les $a \otimes 1_B$ et ceux provenant de B , c'est-à-dire les $1_A \otimes b$, commutent). Maintenant, si $a \in A$ et toujours $m \in M$, on a $\bar{p}(am) = \sum_i a'_i p(a''_i am)$. Mais $\sum_i a'_i \otimes a''_i a = \sum_i a a'_i \otimes a''_i$, ce qui signifie que pour toute application K -bilinéaire $\varphi: A \times A \rightarrow V$ on a $\sum_i \varphi(a'_i, a''_i a) = \sum_i \varphi(a a'_i, a''_i)$, et en particulier en appliquant ça à $\varphi: A \times A \rightarrow M$ envoyant (u, v) sur $up(vm)$, on a $\sum_i a'_i p(a''_i am) = \sum_i a a'_i p(a''_i m)$, soit $\bar{p}(am) = a \bar{p}(m)$.

Si M' est un sous-module de M et $p: M \rightarrow M'$ une rétraction, alors pour $m \in M'$ on a $\bar{p}(m) = \sum_i a'_i p(a''_i m) = \sum_i a'_i a''_i m = m$ puisque l'élément ρ vérifie $\mu(\rho) = 1$ c'est-à-dire précisément $\sum_i a'_i a''_i = 1_A$.

(f) Soit M un $A \otimes_K B$ -module et M' un sous-module : on va montrer que M' admet un supplémentaire dans M ; or ceci revient à trouver une rétraction $A \otimes_K B$ -linéaire $M \rightarrow M'$. Mais puisque B est supposée semi-simple, on sait qu'il existe une rétraction B -linéaire $p: M \rightarrow M'$. La question précédente montre alors précisément que $\bar{p}$ est une rétraction $A \otimes_K B$ -linéaire.

(g) Il suffit de montrer que si A est semi-simple alors A^{op} l'est. On va donc montrer que tout sous- A^{op} -module de A^{op} admet un supplémentaire.

Pour cela, on introduit le K -espace vectoriel DA dual de A , qu'on munit d'une structure de A -module (à gauche) en posant $(af)(b) = f(ba)$ si f est une forme K -linéaire sur A . Si $M \subseteq A$ est un sous- K -espace vectoriel on lui associe le sous- K -espace vectoriel $M^\perp \subseteq DA$ défini par $M^\perp = \{f \in DA : f|_M = 0\}$: on sait bien que $M^\perp$ détermine M (comme l'ensemble des $x \in A$ tels que $f(x) = 0$ pour tout $f \in M^\perp$), que tout sous- K -espace vectoriel de DA s'obtient de la sorte, et que l'application $M \mapsto M^\perp$ est décroissante (inverse les inclusions) et transforme intersections en sommes et réciproquement. Or si M est un sous- A^{op} -module de A^{op} , ou, ce qui revient au même, un sous- A -module à droite de A , alors $M^\perp$ est un sous-

A -module (à gauche) de DA puisque pour $x \in M$ et $f \in M^\perp$ on a $(af)(x) = f(xa) = 0$ si $a \in A$ (vu que $xa \in M$); et réciproquement, si $M^\perp$ est un sous- A -module (à gauche) de DA alors M est un sous- A -module à droite de A puisque pour $x \in M$ et $f \in M^\perp$ on a $f(xa) = (af)(x) = 0$ si $a \in A$ (et car $M^\perp$ détermine M comme rappelé ci-dessus). À présent, si M est un sous- A^{op} -module de A^{op} , ou plutôt un sous- A -module à droite de A , le sous- A -module $M^\perp$ de DA admet un supplémentaire $DA = M^\perp \oplus Q$, et on peut écrire $Q = N^\perp$, où N est un sous- A -module à droite de A , et $DA = M^\perp \oplus N^\perp$ assure $M \oplus N = A$. On a donc bien prouvé que A^{op} est semi-simple.

(h) Si A est séparable, on a vu en (f) que $A \otimes_K B$ est semi-simple pour toute K -algèbre semi-simple B , et d'après la question précédente en particulier $A \otimes_K A^{\text{op}}$ est semi-simple. Il reste donc à expliquer pourquoi la semi-simplicité de $A \otimes_K A^{\text{op}}$ implique la séparabilité de A .

Si $A \otimes_K A^{\text{op}}$ est semi-simple, considérons la structure de $A \otimes_K A^{\text{op}}$ -module sur A donnée par $(a \otimes b)x = axb$ (ceci revient à considérer A comme un (A, A) -bimodule de la façon évidente). Alors l'application $\check{\mu}: A \otimes_K A^{\text{op}} \rightarrow A$ donnée par $a \otimes b \mapsto ab$ est $A \otimes_K A^{\text{op}}$ -linéaire, et elle est manifestement surjective : puisque $A \otimes_K A^{\text{op}}$ est supposé semi-simple, il existe donc une section $\check{\sigma}: A \rightarrow A \otimes_K A^{\text{op}}$ (c'est-à-dire qu'on a $\check{\mu}\check{\sigma} = \text{id}_A$) qui soit $A \otimes_K A^{\text{op}}$ -linéaire, donc vérifiant $\check{\sigma}(axb) = (a \otimes b)\check{\sigma}(x)$: or si on considère $\sigma: A \rightarrow A \otimes_K A$ au lieu de $\check{\sigma}: A \rightarrow A \otimes_K A^{\text{op}}$ (en identifiant A^{op} à A comme K -espace vectoriel), il vérifie cette fois $\sigma(axb) = a\sigma(x)b$ — c'est précisément la propriété par laquelle on a défini la séparabilité. ✓