

# Exercices Algèbre - Modules II

**EXERCICE 1.**

1. Montrer que les groupes

$$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$

sont isomorphes.

2. Montrer qu'un groupe abélien fini non cyclique possède un sous-groupe isomorphe à  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$  pour un certain nombre premier  $p$ .
3. Combien y a-t-il de groupes abéliens de cardinal 360? Plus généralement de cardinal  $n$  avec  $n \geq 1$  un entier naturel?
4. Quels sont les entiers  $n$  tels que le groupe  $(\mathbb{Z}/n\mathbb{Z})^\times$  soit cyclique? Décomposer le groupe  $G = (\mathbb{Z}/187\mathbb{Z})^\times$  sous la forme donnée par le théorème de structure des groupes abéliens de type fini.

**SOLUTION.**

1. Par le théorème chinois, ces deux groupes sont isomorphes à

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}).$$

Il s'agit de l'écriture en composantes  $p$ -primaires tandis que l'écriture en facteurs invariants est

$$\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/900\mathbb{Z}.$$

2. On utilise le théorème de structure des groupes abéliens finis qui garantit que

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}$$

pour un certain  $r \in \mathbb{N}$  et  $d_i \geq 2$  pour  $i \in \{1, \dots, r\}$  et  $d_i \mid d_{i+1}$  pour  $i \in \{1, \dots, r-1\}$ . Comme  $G$  n'est pas cyclique, on a  $r \geq 2$  et pour  $p \mid d_1$  premier,  $p \mid d_i$  pour tout  $i \in \{1, \dots, r\}$ . On sait alors que  $\mathbb{Z}/p\mathbb{Z}$  est un sous-groupe de  $\mathbb{Z}/d_i\mathbb{Z}$  pour tout  $i \in \{1, \dots, r\}$ . On obtient ainsi un sous-groupe de  $G$  isomorphe à  $(\mathbb{Z}/p\mathbb{Z})^r$  qui contient évidemment une copie de  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ .

3. On a  $360 = 2^3 \times 3^2 \times 5$ . La composante 2-primaire d'un tel groupe (à isomorphisme près) est donc un groupe abélien d'ordre 8, à savoir  $\mathbb{Z}/8\mathbb{Z}$ ,  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$  ou  $(\mathbb{Z}/2\mathbb{Z})^3$ . De même, la composante 3-primaire est isomorphe à  $\mathbb{Z}/9\mathbb{Z}$  ou  $(\mathbb{Z}/3\mathbb{Z})^2$  et la composante 5-primaire est isomorphe à  $\mathbb{Z}/5\mathbb{Z}$ . On obtient ainsi 6 classes d'isomorphismes de groupes abéliens de cardinal 360, à savoir

$$\begin{aligned} \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} &\cong \mathbb{Z}/360\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z} \\ (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} &\cong (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/90\mathbb{Z} \\ \mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} &\cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z} \\ (\mathbb{Z}/2\mathbb{Z})^3 \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}. \end{aligned}$$

Dans le cas général, si  $n = \prod_{i=1}^r p_i^{\alpha_i}$  avec  $r \in \mathbb{N}^\times$ ,  $p_1, \dots, p_r$  des nombres premiers distincts et  $\alpha_i \geq 1$ . Par le théorème de structure, on sait que les classes d'isomorphismes de groupes abéliens d'ordre  $n$  sont caractérisées par la liste des facteurs invariants  $(d_1, \dots, d_s)$  pour un certain  $s \in \mathbb{N}$  et  $d_i \geq 2$  pour  $i \in \{1, \dots, s\}$  et  $d_i \mid d_{i+1}$  pour  $i \in \{1, \dots, s-1\}$  et  $d_1 \cdots d_s = n$ . Par conséquent, chaque  $d_i$  se décompose sous la forme  $d_i = p_1^{\alpha_{i,1}} \cdots p_r^{\alpha_{i,r}}$  avec les contraintes que pour

tout  $i \in \{1, \dots, s-1\}$  et tout  $j \in \{1, \dots, r\}$ ,  $\alpha_{i,j} \leq \alpha_{i+1,j}$  et  $\sum_{i=1}^s \alpha_{i,j} = \alpha_j$ . Il s'ensuit que le nombre de choix possibles

est de  $\prod_{j=1}^r p(\alpha_j)$  où  $p(\cdot)$  désigne la fonction nombre de partitions croissantes d'entiers strictement positifs.

4. On pose  $n = \prod_p p^{\alpha_p}$  la décomposition de  $n$  en produit de facteurs premiers. On sait alors d'après le cours que

$$(\mathbf{Z}/n\mathbf{Z})^\times \cong (\mathbf{Z}/2^{\alpha_2}\mathbf{Z})^\times \times \prod_{\substack{p \neq 2 \\ \alpha_p \geq 1}} \mathbf{Z}/p^{\alpha_p-1}(p-1)\mathbf{Z}$$

Or, on sait que

$$(\mathbf{Z}/2^{\alpha_2}\mathbf{Z})^\times = \begin{cases} \{0\} & \text{si } \alpha_2 = 1 \\ \mathbf{Z}/2\mathbf{Z} & \text{si } \alpha_2 = 2 \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{\alpha_2-2}\mathbf{Z} & \text{si } \alpha_2 \geq 3. \end{cases}$$

Un groupe cyclique ne pouvant contenir plus d'un élément, d'ordre 2, on voit que  $(\mathbf{Z}/n\mathbf{Z})^\times$  est cyclique si, et seulement si,  $n = p^\alpha$  ou  $n = 2p^\alpha$  avec  $p$  un nombre premier impair et  $\alpha \geq 0$  ou  $n = 4$ .

Pour finir, on a  $187 = 11 \times 17$  de sorte que

$$(\mathbf{Z}/187\mathbf{Z})^\times \cong \mathbf{Z}/10\mathbf{Z} \times \mathbf{Z}/16\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/80\mathbf{Z}.$$

**EXERCICE 2.**

Soit  $K$  un corps. Soit  $E$  un  $K$ -espace vectoriel de dimension finie non nulle. Soit  $u$  un endomorphisme de  $E$ . On dit que  $u$  est cyclique s'il existe une base dans laquelle sa matrice est une matrice compagnon  $C(P)$ , où  $P$  est un polynôme.

1. Montrer que  $u$  est cyclique si, et seulement si, son polynôme minimal est égal à son polynôme caractéristique.
2. Montrer que  $u$  est cyclique si, et seulement si, les seuls endomorphismes qui commutent avec  $u$  sont les polynômes en  $u$ .
3. On dit que  $u$  est irréductible si les seuls sous-espaces de  $E$  stables par  $u$  sont  $E$  et  $\{0\}$ . Montrer que  $u$  est irréductible si, et seulement si, il est cyclique et son polynôme caractéristique est irréductible.

On dit que  $u$  est semi-simple si tout sous-espace vectoriel  $F$  stable par  $u$  admet un supplémentaire stable par  $u$ .

4. Montrer que  $u$  est semi-simple si, et seulement si, son polynôme minimal est sans facteur carré. En déduire que si  $u$  est diagonalisable, alors  $u$  est semi-simple. Que dire dans le cas d'un corps algébriquement clos?  
Indication : On pourra munir  $(E, u)$  d'une structure de  $k[X]/(\pi_u)$ -module où  $\pi_u$  est le polynôme minimal de  $u$ .
5. Montrer que si  $K$  est de caractéristique nulle, alors  $u$  est semi-simple si, et seulement si, il existe une extension  $L$  de  $K$  sur laquelle  $u$  est diagonalisable.

**SOLUTION.**

1. On sait qu'il existe une base dans laquelle la matrice de  $u$  est du type  $\text{diag}(C(P_1), \dots, C(P_r))$ , où  $C(P_i)$  est la matrice compagnon du polynôme  $P_i$ , avec  $P_1 | P_2 | \dots | P_r$ . Comme le polynôme minimal de  $u$  est  $P_r$  et que son polynôme caractéristique est  $\prod_{i=1}^r P_i$ , la condition que ces deux polynômes soient égaux équivaut au fait que  $r = 1$ , i.e. qu'il existe une base dans laquelle la matrice de  $u$  est une matrice compagnon.
2. Si  $u$  est cyclique, on a une base de  $E$  du type  $(x, u(x), \dots, u^{n-1}(x))$  (en prenant une base dans laquelle la matrice de  $u$  est une matrice compagnon). Si  $v$  commute avec  $u$ , on décompose  $v(x)$  dans cette base, soit

$$v(x) = \sum_{k=0}^{n-1} a_k u^k(x),$$

où les  $a_i$  sont dans  $K$ . Posons  $P = \sum_{k=0}^{n-1} a_k X^k$ , alors  $v(x) = P(u)(x)$ , d'où on tire

$$v(u^k(x)) = u^k(v(x)) = P(u)(u^k(x))$$

puisque  $v$  commute avec  $u$ . Ceci étant vrai pour tout  $k \in \mathbf{N}$ , on a donc  $v = P(u)$  car  $(x, u(x), \dots, u^{n-1}(x))$  est une base de  $E$ .

Si maintenant  $u$  n'est pas cyclique, il existe une base dans laquelle sa matrice est du type  $M = \text{diag}(C(P_1), \dots, C(P_r))$  (cf. 1., avec  $r \geq 2$ ). En particulier, la matrice de la forme  $N = \text{diag}(1, 1, \dots, 1, 0)$  commute avec  $M$ . Or, si  $N$  s'écrivait  $N = Q(M)$  où  $Q$  est un polynôme, on aurait  $Q(C(P_r)) = 0$ , donc  $Q$  serait multiple de  $P_r$  car  $P_r$  est le polynôme minimal de  $C(P_r)$ . Alors tous les  $P_i$  divisent  $P_r$  d'où  $Q(C(P_i)) = 0$  car  $P_i$  est le polynôme minimal de  $C(P_i)$ . On aboutit à  $N = Q(M) = 0$ , d'où une contradiction.

3. Si  $u$  a un espace stable autre que  $\{0\}$  et  $E$ , il est immédiat (par exemple en écrivant la matrice par blocs de  $u$ ) que le polynôme caractéristique  $P$  n'est pas irréductible. Supposons réciproquement que  $u$  n'ait pas de sous-espaces stables non triviaux. En écrivant la matrice de  $u$  dans une certaine base sous la forme  $M = \text{diag}(C(P_1), \dots, C(P_r))$  comme ci-dessus, on voit qu'on doit avoir  $r = 1$  (sinon le sous-espace engendré par les  $(\deg P_1)$  premiers vecteurs de la base serait stable et non égal à  $\{0\}$  ou  $E$ ), on a donc  $u$  cyclique, de matrice  $C(P)$ . Si maintenant  $P = QR$  avec  $Q$  et  $R$  premiers entre eux et non constants, alors le lemme des noyaux dit que  $E$  est somme directe des sous-espaces  $\text{Ker}(Q(u))$  et  $\text{Ker}(R(u))$  qui sont non triviaux vu que le polynôme minimal de  $C(P)$  est  $P$ . Reste à écarter le cas où  $P = Q^r$  avec  $Q$  irréductible et  $r \geq 2$ , mais dans ce cas  $\text{Ker}(Q(u))$  est un sous-espace stable non trivial puisque  $Q(u)$  est non inversible (vu que  $P(u) = 0$ ) et distinct de  $E$  (puisque  $Q(u) \neq 0$ , le polynôme minimal de  $u$  étant  $Q^r$ ).
4. Supposons que  $u$  soit semi-simple et raisonnons par l'absurde en supposant que  $\pi_u$ , le polynôme minimal de  $u$ , n'est pas sans facteur carré. Il existe alors  $P$  unitaire constant et  $Q$  tels que  $\pi_u = P^2Q$ . Le sous-espace vectoriel  $F = \text{Ker}(P(u))$  est alors stable<sup>1</sup> par  $u$  et par semi-simplicité, il existe  $G$  stable par  $u$  tel que  $E = F \oplus G$ . On a alors que  $(PQ)(u)$  s'annule sur  $G$ . De la relation  $P \times PQ = \pi_u$ , on tire que  $P(u) \circ (PQ)(u)(G) = \{0\}$  soit que  $(PQ)(u)(G) \subseteq F$ . Mais par stabilité,  $(PQ)(u)(G) \subseteq G$  et comme  $F$  et  $G$  sont supplémentaires, on a le résultat. Mais on a aussi  $(PQ)(u)(F) = Q(u) \circ P(u)(F) = \{0\}$  si bien que  $PQ$  est annulateur de  $u$  de degré strictement inférieur à  $\pi_u$ , ce qui est absurde. Finalement  $\pi_u$  est sans facteurs carrés.

Réciproquement, supposons  $\pi_u$  irréductible. On sait alors que  $(E, u)$  est un  $k[X]$ -module et justifions que  $(E, u)$  puisse être muni d'une structure de  $k[X]/(\pi_u)$ -module. Montrons en réalité le résultat plus général suivant. Soit  $A$  un anneau commutatif et  $I$  un idéal de  $A$ . Alors on a une correspondance entre les  $A$ -modules  $M$  vérifiant  $IM = \{0\}$  et les  $A/I$ -modules. Soit dans un premier temps un  $A/I$ -module  $M$  et montrons qu'il s'agit d'un  $A$ -module vérifiant  $IM = \{0\}$ . On note  $\pi : A \rightarrow A/I$  la surjection canonique et on voit immédiatement qu'on a une structure de  $A$ -module grâce à

$$\forall (a, m) \in A \times M, \quad a \cdot m = \pi(a) \cdot m.$$

En particulier, on a bien pour tout  $i \in I$  et  $m \in M$  que  $im = 0$ , soit que  $IM = \{0\}$ . Réciproquement, si  $M$  est un  $A$ -module tel que  $IM = \{0\}$ , alors le morphisme d'anneaux

$$\Theta_M : \begin{cases} A & \longrightarrow & \text{End}_{\text{Gr}}(M) \\ a & \longmapsto & [m \mapsto a \cdot m] \end{cases}$$

est nul sur  $I$  et passe au quotient pour donner un unique morphisme  $\tilde{\Theta}_M$  vérifiant  $\tilde{\Theta}_M \circ \pi = \Theta_M$  et on vérifie que  $\tilde{\Theta}_M$  munit  $M$  d'une structure de  $A/I$ -module. En d'autres termes, pour tout  $x \in A/I$  tel que  $x = \pi(a)$  avec  $a \in A$ , alors pour tout  $m \in M$

$$x \cdot m = \tilde{\Theta}_M(x)(m) = \theta_M(a)(m) = a \cdot m$$

et cela est indépendant du choix du représentant.

Revenons-en à l'exercice et considérons  $(E, u)$  muni de cette structure de  $k[X]/(\pi_u)$ -module, ce qui est possible car pour tout  $x \in E$ ,  $\pi_u \cdot x = \pi_u(u)(x) = 0$ . Dans ce cas,  $k[X]/(\pi_u)$  est un corps et donc cette structure fournit une structure d'espace vectoriel sur ce corps, que l'on notera  $K$ . Soit alors  $F$  un sous-espace stable par  $u$ . En particulier,  $F$  est un sous- $K$ -espace vectoriel et par le théorème de la base incomplète, on peut choisir un supplémentaire  $G$  à  $F$  dans  $E$ . On a ainsi  $E = F \oplus G$ . Mais  $G$  est alors un  $k$ -espace vectoriel et le fait qu'il soit aussi un  $K$ -espace vectoriel nous indique qu'il est stable par  $u$  car c'est un  $k[X]/(\pi_u)$ -module donc en particulier un sous- $k[X]$ -module qui correspond à un sous-espace stable. On a donc bien la semi-simplicité de  $u$ . Voyons à présent comment nous ramener au cas irréductible. Supposons  $\pi_u$  sans facteur carré et que  $\pi_u = Q_1 \cdots Q_r$  avec les  $Q_i$  irréductibles deux à deux non associés. Par le lemme des noyaux, on a donc

$$E = \bigoplus_{i=1}^r F_i \quad \text{avec} \quad F_i = \text{Ker}(Q_i(u)).$$

1. En effet, si  $x \in F$ , alors  $P(u)(x) = 0$  et  $P(u)(u(x)) = P(u) \circ u(x) = u \circ P(u)(x) = 0$ .

Le même lemme des noyaux appliqué à  $u|_F$  et au polynôme<sup>2</sup>  $\pi_u$  donne aussi

$$F = \bigoplus_{i=1}^r F_i \cap F.$$

Par ailleurs,  $Q_i$  est le polynôme minimal de  $u|_{F_i}$  car il annule cet endomorphisme et est irréductible. D'après ce qui précède,  $u|_{F_i}$  est semi-simple et comme  $F \cap F_i$  est stable, il existe un supplémentaire  $G_i$  de  $F \cap F_i$  dans  $F_i$ . Ce supplémentaire est stable par  $u|_{F_i}$  donc par  $u$  et finalement

$$G = \bigoplus_{i=1}^r G_i$$

est un supplémentaire stable par  $u$  de  $F$  et  $u$  est semi-simple. On a donc bien établi l'équivalence!

Le fait que  $u$  soit diagonalisable est équivalent au fait que son polynôme minimal soit scindé à racines simples<sup>3</sup> (donc en particulier sans facteurs carrés) et  $u$  est donc semi-simple.

Sur un corps algébriquement clos, les notions de semi-simplicité et de diagonalisabilité coïncident. On vient de voir que diagonalisable impliquait semi-simple en général. Supposons alors que  $u$  soit semi-simple. On vient de voir que cela implique que  $\chi_u$  est sans facteur carré et comme un polynôme unitaire irréductible sur un corps algébriquement clos est de la forme  $X - \lambda$  pour  $\lambda \in k$ , on en déduit que  $\chi_u$  est de la forme

$$\chi_u = \prod_{i=1}^s (X - \lambda_i) \quad \lambda_1, \dots, \lambda_s \in k.$$

Ainsi, il est scindé à racines simples et  $u$  est diagonalisable.

5. Soient  $k \subseteq K$  deux corps et  $U \in \mathcal{M}_n(k)$ . On a alors que le polynôme minimal de  $U$  vue dans  $\mathcal{M}_n(k)$  ou dans  $\mathcal{M}_n(K)$  est le même (voir la note de bas de page 20). Il suffit donc de montrer qu'un polynôme à coefficients dans  $k$  est sans facteur carré dans  $k[X]$  si, et seulement si, il l'est dans  $K[X]$ . On voit aisément qu'en caractéristique nulle, un polynôme est sans facteur carré<sup>4</sup> si, et seulement si,  $\text{pgcd}(P, P') = 1$ . On conclut alors grâce à la première question de l'exercice 15 du TD IV. Finalement  $u$  est semi-simple sur  $k$  si, et seulement si, elle l'est sur  $K$ . Il suffit alors de considérer pour  $K$  un corps de décomposition du polynôme minimal de  $u$  sur lequel (puisque  $\pi_u$  est scindé), semi-simple équivaut à diagonalisable.

**EXERCICE 3.** Soient  $M$  et  $N$  deux  $A$ -modules.

1. Soit  $f : M \otimes_A N \rightarrow P$  un morphisme. Si  $f(m \otimes n) = 0$  implique  $m \otimes n = 0$  pour tous  $m \in M$  et  $n \in N$ , l'application  $f$  est-elle injective?  
*Indication : On pourra considérer  $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C} \rightarrow \mathbf{C}$  définie par  $z \otimes w \mapsto zw$ .*
2. Trouver un exemple tel que  $M \otimes_A M = M$ ?  $M \otimes_A M = \{0\}$ ?
3. Si  $M$  est sans torsion,  $M \otimes_A M$  est-il sans torsion?

2. Le polynôme minimal de  $u|_F$  divise  $\pi_u$  donc est produit de certains  $Q_i$ .

3. Ce qui peut se retrouver en remarquant qu'une diagonalisation est une réduction de Jordan et on en déduit alors les invariants de similitudes mais peut aussi se démontrer de façon élémentaire grâce au lemme des noyaux.

4. En effet, si  $P = \prod_{i=1}^d P_i^{\ell_i}$  est la décomposition de  $P$  en produits d'irréductibles 2 à 2 non associés, on a

$$\text{pgcd}(P, P') = \prod_{i=1}^d P_i^{\ell_i - 1}.$$

Il est clair que ce pgcd est de la forme  $\prod_{i=1}^d P_i^{\mu_i}$  avec  $\mu_i \leq \ell_i$ . Par ailleurs, pour tout  $i \in \{1, \dots, r\}$ ,  $P = P_i^{\ell_i} Q_i$  avec  $P_i$  et  $Q_i$  premiers entre eux. On a en dérivant

$$P' = \ell_i P_i^{\ell_i - 1} P_i' Q_i + P_i^{\ell_i} Q_i' = P_i^{\ell_i - 1} (\ell_i P_i' Q_i + P_i Q_i')$$

et on en déduit que  $P_i$  est de multiplicité  $\mu_i$  est au moins  $\ell_i - 1$  dans  $\text{pgcd}(P, P')$ . Par ailleurs, elle vaut  $\ell_i$  si, et seulement si,  $P_i \mid \ell_i P_i' Q_i$  soit (par le lemme de Gauß) si, et seulement si,  $P_i \mid P_i'$  mais en caractéristique nulle c'est impossible pour des raisons de degré. On en déduit que  $\mu_i = \ell_i - 1$  et le résultat. En caractéristique  $p$ , il peut arriver des phénomènes différents du fait de polynômes de la forme  $P(X^p)$  de dérivée nulle (voir Proposition 5.39 du Beck, Malick, Peyré).

**SOLUTION.**

- Non en général! Le fait que  $f(m \otimes n) = 0$  implique que  $m \otimes n = 0$  n'implique pas l'injectivité car on n'a pas que des tenseurs purs et la propriété d'être dans le noyau n'a rien d'additif. On peut par exemple considérer l'application<sup>5</sup>  $f : \mathbf{C} \otimes_{\mathbf{R}} \mathbf{C} \rightarrow \mathbf{C}$  définie par  $z \otimes w \mapsto zw$ . Il est clair que  $f(z \otimes w) = 0$  implique  $z = 0$  ou  $w = 0$  donc  $z \otimes w = 0$  mais l'application n'est pas injective car

$$f(1 \otimes i - i \otimes 1) = i - i = 0$$

mais  $1 \otimes i \neq i \otimes 1$  car par exemple une  $\mathbf{R}$ -base de  $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C}$  est donnée par  $1 \otimes 1, 1 \otimes i, i \otimes 1, i \otimes i$  par le cours. On pouvait aussi considérer l'application  $\mathbf{R}$ -bilinéaire  $\mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$  définie par  $(z_1, z_2) \mapsto \overline{z_1}z_2$  par laquelle  $(i, 1)$  est envoyé sur  $-i$  et  $(1, i)$  sur  $i$ .

Cela dit, parfois il est possible d'étudier le noyau comme on le verra mais en général, il est plus simple de construire un inverse à gauche  $g$  tel que  $g \circ f = \text{Id}$  ce qui établit l'injectivité et se vérifie en établissant que  $g(f(m \otimes n)) = m \otimes n$  qui est bien dans ce cas une propriété additive qu'il suffit de vérifier sur les générateurs que sont les tenseurs purs.

- On a par exemple pour tout anneau intègre  $A$  de corps de fraction  $k$ , que  $k \otimes_A k = k$  (voir exercice 7, question 1.). On a alors au vu de la discussion ci-dessus que pour que  $M \otimes_A M = \{0\}$  dans le cas de groupes abéliens, qu'il est nécessaire de choisir  $M$  de torsion et divisible<sup>6</sup>. Considérons alors par exemple  $\mathbf{Q}/\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Q}/\mathbf{Z}$ . On a alors pour tous  $\overline{x}, \overline{y} \in \mathbf{Q}/\mathbf{Z}$  l'existence d'un entier  $n \geq 1$  tel que  $n\overline{x} = \overline{0}$  si bien que

$$\overline{x} \otimes \overline{y} = \overline{x} \otimes \left( n \cdot \frac{\overline{y}}{n} \right) = (n\overline{x}) \otimes \left( \frac{\overline{y}}{n} \right) = 0$$

et on conclut du fait que les tenseurs purs engendrent  $\mathbf{Q}/\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Q}/\mathbf{Z}$  que  $\mathbf{Q}/\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Q}/\mathbf{Z} = \{0\}$ .

On peut établir que si  $M$  est de type fini,  $M^{\otimes k} \neq \{0\}$  pour tout entier  $k$ . Soient  $x_1, \dots, x_n$  un système minimal de générateurs de  $M$  et on pose  $M = N + x_n A$  avec  $N = \langle x_1, \dots, x_{n-1} \rangle$  (on pose  $\{0\}$  si  $n = 1$ ). On a  $x_n \notin N$  et  $I = \{a \in A : ax_n \in N\}$  est un idéal de  $A$  qui ne contient pas 1 donc propre. Tout élément  $m \in M$  est de la forme  $m = n + ax_n$  avec  $n \in N$  et  $a \in A$ . La valeur de  $a$  n'est pas unique mais elle le devient modulo  $I$  car si  $n + ax_n = n' + a'x_n$  alors  $(a - a')x_n \in N$  si bien que  $a \equiv a' \pmod{I}$  et que  $M^k \rightarrow A/I$  donnée par

$$(n_1 + a_1 x_n, \dots, n_n + a_n x_n) \mapsto a_1 \cdots a_n \pmod{I}$$

est bien définie et  $k$ -multilinéaire de sorte qu'elle donne lieu à une application linéaire  $M^{\otimes k} \rightarrow A/I$  telle que  $x_n \otimes \cdots \otimes x_n \mapsto 1$  si bien que  $M^{\otimes k} \neq \{0\}$ .

- Posons  $I = (X, Y)$  dans  $A = k[X, Y]$  avec  $k$  un corps. Il est clair que  $I$  est un  $A$ -module sans torsion. Étudions alors  $I \otimes_A I$ . On a<sup>7</sup>

$$X(X \otimes Y) = X \otimes (XY) = Y(X \otimes X)$$

et de même  $X(Y \otimes X) = Y(X \otimes X)$  de sorte que dans  $I \otimes_A I$ , on ait

$$X(X \otimes Y - Y \otimes X) = 0$$

mais  $X \otimes Y - Y \otimes X \neq 0$ . En effet, considérons l'application bilinéaire<sup>8</sup>  $f : I \times I \rightarrow k$  définie par

$$(f, g) \mapsto \partial_X f(0, 0) \partial_Y g(0, 0).$$

Cette application donne lieu à une unique application linéaire  $\tilde{f} : I \otimes_A I \rightarrow k$  telle que  $\tilde{f}(X \otimes Y) = 1$  tandis que  $\tilde{f}(Y \otimes X) = 0$  ce qui implique nécessairement que  $X \otimes Y - Y \otimes X \neq 0$ .

**EXERCICE 4.**

5. Qui provient par propriété universelle du produit tensorielle de l'application  $\mathbf{R}$ -bilinéaire  $\mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$  définie par  $(z_1, z_2) \mapsto z_1 z_2$ .  
 6. Noter qu'un module divisible ne peut être de type fini d'après le DM I car un tel module n'admet pas de sous-groupe maximal tandis que tout groupe de type fini en admet au moins un.  
 7. Attention qu'on a pas  $X \otimes Y = (XY)(1 \otimes 1)$  car  $1 \notin I$ ! En revanche, dans  $A^{\otimes 2}$ , on a bien  $X \otimes Y = Y \otimes X = (XY)(1 \otimes 1)$ .  
 8. Ici, on a besoin de voir  $k$  comme un  $k[X, Y]$  module et pour ce faire, on peut définir la multiplication comme la multiplication par le terme constant du polynôme ou de manière équivalente en voyant  $k \cong k[X, Y]/I$ .

- Donner les invariants de similitude et les réduites de Frobenius<sup>9</sup> correspondantes des endomorphismes  $u \in \mathcal{L}(k^4)$  dont le polynôme caractéristique est  $\chi_u = X^4$  dans les cas suivants :  $k = \mathbf{F}_2$ ,  $k = \mathbf{Q}$  et  $k = \mathbf{C}$ .
- Même question avec  $\chi_u = X(X-1)(X-2)(X-3)$  et  $u \in \mathcal{L}(k^6)$  et  $\chi_u = (X^2+1)(X^2+X+1)^2$ .
- Démontrer que toute matrice à coefficients dans  $k$  algébriquement clos est conjuguée à une matrice diagonale par blocs où chaque bloc est de la forme  $J_n(\lambda)$ .  
Indication : Considérer la multiplication par la classe de  $X$  dans  $k[X]/((X-\lambda)^n)$  dans la base  $1, X-\lambda, (X-\lambda)^2, \dots, (X-\lambda)^{n-1}$ .
- Que se passe-t-il dans le cas  $k = \mathbf{R}$ ?
- Prendre les questions 1. et 2. avec les réduites de Jordan et  $k = \mathbf{C}$ .
- Donner les réduites de Jordan des endomorphismes  $u \in \mathcal{L}(\mathbf{C}^4)$  dont les invariants de similitudes sont :
  - $P_1 = X(X-1)$  et  $P_2 = X(X-1)$ ;
  - $P_1 = X-1$  et  $P_2 = X^2(X-1)$ ;
  - $P_1 = X$  et  $P_2 = X(X-1)^2$ ;
  - $P_1 = X^2(X-1)^2$ .
- Donner les invariants de similitude des matrices (avec  $k$  de caractéristique nulle)

$$U = \text{diag}(J_3(1), J_2(1), J_2(0), 0), \quad V = \text{diag}(J_2(1), 1, J_2(2), J_2(2), J_3(2)) \quad \text{et} \quad W = \text{diag}(1, 1, 1, 2, 2)$$

avec

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & & & \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda \end{pmatrix}^T.$$

- Calculer les invariants de similitude des matrices

$$\begin{pmatrix} X^2-1 & X(X-1) & (X-1)(X-5) \\ (X-1)(X^2+3X+2) & X^2-3X+2 & (X-1)^3 \end{pmatrix} \in \mathcal{M}_{2,3}(\mathbf{Q}[X]) \quad \text{et} \quad \begin{pmatrix} 3 & 2 & -2 \\ -1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbf{Q}).$$

**SOLUTION.**

- Commençons par quelques généralités. On note  $P_1 \mid \dots \mid P_s$  pour  $s \in \mathbf{N}^\times$  la suite des invariants de similitude de  $u$ . Par définition, on a  $\prod_{i=1}^s P_i = \chi_u$  et  $P_i \mid P_s$  pour tout  $i \in \{1, \dots, s\}$  si bien que  $P_s$  est divisible par le produit des facteurs irréductibles de  $\chi_u$ . Autrement dit, si

$$\chi_u = \prod_{i=1}^t Q_i^{\alpha_i}$$

est la décomposition de  $\chi_u$  en produit de polynômes  $Q_1, \dots, Q_t$  de  $k[X]$  irréductibles 2 à 2 non associés et  $\alpha_1, \dots, \alpha_t \in \mathbf{N}^\times$ , alors

$$P_s = \prod_{i=1}^t Q_i^{\beta_i} \quad \text{avec} \quad \forall i \in \{1, \dots, t\}, \quad 1 \leq \beta_i \leq \alpha_i.$$

On peut alors itérer ce procédé puisque

$$\prod_{i=1}^{s-1} P_i = \prod_{i=1}^t Q_i^{\alpha_i - \beta_i} \quad \text{et} \quad \forall i \in \{1, \dots, s-1\}, \quad P_i \mid P_{s-1}$$

9. Autrement dit, la matrice du Théorème 3.18 des notes de cours.

si bien que de même

$$P_{s-1} = \prod_{i=1}^t Q_i^{\gamma_i} \text{ avec } \forall i \in \{1, \dots, t\}, 0 \leq \gamma_i \leq \min(\beta_i, \alpha_i - \beta_i) \text{ et } \gamma_i \geq 1 \text{ si } \alpha_i - \beta_i > 0.$$

En effet, la condition  $\gamma_i \leq \beta_i$  traduit que  $P_{s-1} \mid P_s$  et  $\gamma_i \leq \alpha_i - \beta_i$  traduit que  $P_{s-1} \mid \frac{\chi_u}{P_s}$  tandis que si  $\alpha_i - \beta_i > 0$ , la condition  $\gamma_i \geq 1$  traduit le fait que pour tout  $i \in \{1, \dots, s-1\}$ ,  $P_i \mid P_{s-1}$ . On peut alors itérer le procédé jusqu'à  $P_1$ .

Mettons cet algorithme en pratique. Ici,  $\chi_u = X^4$  qui n'admet sur tous les corps proposé un unique facteur irréductible, à savoir  $X$ . On a donc 4 possibilités pour  $P_s$ .

- Soit  $P_s = X^4$  auquel cas nécessairement  $s = 1$  et on a un unique invariant de similitude  $P_1 = \chi_u$ ;
- Soit  $P_s = X^3$  et alors  $s = 2$  et  $P_1 = X$  et on a deux invariants de similitude  $P_1 = X$  et  $P_2 = X^3$ ;
- Soit  $P_s = X^2$  et alors soit  $s = 2$  et  $P_1 = X^2$  et on a deux invariants de similitude  $P_1 = X^2$  et  $P_2 = X^2$  soit  $s = 3$  et  $P_2 = P_1 = X$  et on a trois invariants de similitude  $P_1 = P_2 = X$  et  $P_3 = X^2$ ;
- Soit  $P_s = X$  et nécessairement  $s = 4$  et on a 4 invariants de similitudes  $P_1 = P_2 = P_3 = P_4 = X$ .

Finalement, quel que soit le corps  $k$ , on obtient les résultats suivants :

Invariants de similitude	$X^4$	$X^3, X$	$X^2, X^2$	$X^2, X, X$	$X, X, X, X$
Réduite de Frobenius	$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ & & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 1 & 0 \\ & 0 & 0 \\ & & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 1 & 0 \\ & 0 \\ & & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & & & \\ & 0 & & \\ & & 0 & \\ & & & 0 \end{pmatrix}$

2. Dans le premier cas et en caractéristique nulle (ici  $k = \mathbf{Q}$  ou  $k = \mathbf{C}$ ), on a els facteurs irréductibles  $X, X - 1, X - 2$  et  $X - 3$  si bien que nécessairement  $s = 1$  et  $P_1 = X(X - 1)(X - 2)(X - 3)$  de réduite de Frobenius

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 6 \\ 0 & 1 & 0 & -11 \\ 0 & 0 & 1 & 6 \end{pmatrix} \text{ car } P_1 = X^4 - 6X^3 + 11X^2 - 6X.$$

Dans le cas  $k = \mathbf{F}_2$ , on a  $\chi_u = X^2(X + 1)^2$  et la situation change du fait de ces facteurs multiples. On obtient les facteurs irréductibles  $X$  et  $X + 1$ . On a alors la disjonction de cas suivante :

- Soit  $P_s = X^2(X + 1)^2$  auquel cas  $s = 1$  et on a un unique invariant de similitude qui est  $P_1 = \chi_u$ ;
- Soit  $P_s = X(X + 1)^2$  auquel cas  $s = 2$  et on a deux invariants de similitude qui sont  $P_1 = X$  et  $P_2 = X(X + 1)^2$ ;
- Soit  $P_s = X^2(X + 1)$  auquel cas  $s = 2$  et on a deux invariants de similitude qui sont  $P_1 = X + 1$  et  $P_2 = X^2(X + 1)$ ;
- Soit  $P_s = X(X + 1)$  auquel cas soit  $s = 2$  et on a deux invariants de similitude qui sont  $P_1 = P_2 = X(X + 1)$ .

On aboutit aux résultats suivants :

Invariants de similitude	$X^2(X + 1)^2$	$X(X + 1)^2, X$	$X^2(X + 1), X + 1$	$X(X + 1), X(X + 1)$
Réduite de Frobenius	$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ & & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ & & & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 1 & 1 \\ & 0 & 0 \\ & & 1 & 1 \end{pmatrix}$

Passons à présent au cas de  $u \in \mathcal{L}(k^6)$  et  $\chi_u = (X^2 + 1)(X^2 + X + 1)^2$  et commençons par traiter le cas de  $k = \mathbf{C}$ . Les

facteurs irréductibles sont  $X \pm i, X - j$  et  $X - j^2$ . On obtient alors de même

Invariants de similitude	Réduite de Frobenius
$(X^2 + 1)(X^2 + X + 1)^2$	$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & 0 & -4 \\ 0 & 0 & 1 & 0 & 0 & -4 \\ 0 & 0 & 0 & 1 & 0 & -4 \\ 0 & 0 & 0 & 0 & 1 & -2 \end{pmatrix}$
$(X^2 + 1)(X^2 + X + 1)(X - j), X - j^2$	$\begin{pmatrix} 0 & 0 & 0 & 0 & j \\ 1 & 0 & 0 & 0 & j-1 \\ 0 & 1 & 0 & 0 & 2j-1 \\ 0 & 0 & 1 & 0 & j-2 \\ 0 & 0 & 0 & 1 & j-1 \end{pmatrix} \cdot j^2$
$(X^2 + 1)(X^2 + X + 1)(X - j^2), X - j$	$\begin{pmatrix} 0 & 0 & 0 & 0 & j^2 \\ 1 & 0 & 0 & 0 & j^2-1 \\ 0 & 1 & 0 & 0 & 2j^2-1 \\ 0 & 0 & 1 & 0 & j^2-2 \\ 0 & 0 & 0 & 1 & j^2-1 \end{pmatrix} \cdot j$
$(X^2 + 1)(X^2 + X + 1), X^2 + X + 1$	$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & -1 \\ & & & 0 & -1 \\ & & & & 1 & -1 \end{pmatrix}$

Dans le cas  $k = \mathbf{Q}$ , on obtient les facteurs irréductibles<sup>10</sup>  $X^2 + 1$  et  $X^2 + X + 1$  et ainsi<sup>11</sup> :

Invariants de similitude	Réduite de Frobenius
$(X^2 + 1)(X^2 + X + 1)^2$	$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & 0 & -4 \\ 0 & 0 & 1 & 0 & 0 & -4 \\ 0 & 0 & 0 & 1 & 0 & -4 \\ 0 & 0 & 0 & 0 & 1 & -2 \end{pmatrix}$
$(X^2 + 1)(X^2 + X + 1), X^2 + X + 1$	$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & -1 \\ & & & 0 & -1 \\ & & & & 1 & -1 \end{pmatrix}$

Reste le cas  $k = \mathbf{F}_2$ . Sur  $\mathbf{F}_2[X]$ , on voit que  $X^2 + X + 1$  est irréductible (car sans racine et de degré 2) et donc  $\chi_U =$

10. Car de degré 2 et sans racine rationnelle.

11. Noter qu'on a aussi le résultat suivant qui permet de retrouver ce résultat. Si  $k \subseteq K$  sont deux corps et  $U \in \mathcal{M}_n(k)$ . Alors les invariants de similitude de  $U$  vue dans  $\mathcal{M}_n(k)$  sont aussi les invariants de similitudes de  $U$  vue dans  $\mathcal{M}_n(K)$ , ce qui découle de l'unicité dans le Théorème 3.18 du cours.



$(X + 1)^2(X^2 + X + 1)^2$  et les facteurs irréductibles sont  $X + 1$  et  $X^2 + X + 1$ . On obtient ainsi :

Invariants de similitude	Réduite de Frobenius
$(X + 1)^2(X^2 + X + 1)^2 = X^6 - 1$	$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$
$(X + 1)(X^2 + X + 1)^2, X + 1$	$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ & & & & & 1 \end{pmatrix}$
$(X + 1)^2(X^2 + X + 1), X^2 + X + 1$	$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ & & & & 0 & 1 \\ & & & & 1 & 1 \end{pmatrix}$
$(X + 1)(X^2 + X + 1), (X + 1)(X^2 + X + 1)$	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ & & & 0 & 0 & 1 \\ & & & 1 & 0 & 0 \\ & & & 0 & 1 & 0 \end{pmatrix}$

3. Soit  $M \in \mathcal{M}_n(k)$ . On munit  $k^n$  de la structure de  $k[X]$ -module de type fini du cours<sup>12</sup> associée à  $M$ . Comme  $k$  est un corps algébriquement clos, les polynômes irréductibles unitaires sont exactement les  $X - \lambda$  pour  $\lambda \in k$ . Par le théorème de structure<sup>13</sup>, il vient l'existence de  $r \in \mathbf{N}$ , de  $t \in \mathbf{N}^\times$  et de  $\lambda_1, \dots, \lambda_t$  des éléments distincts de  $k$ , de  $j_i \in \mathbf{N}^\times$  et de d'une famille décroissante d'entiers  $n_{i,1} \geq \dots \geq n_{i,j_i}$  pour tout  $i \in \{1, \dots, t\}$  tels que

$$k^n \cong_{k[X]\text{-mod.}} k[X]^r \oplus \left( \bigoplus_{i=1}^t \bigoplus_{j=1}^{j_i} k[X]/\langle (X - \lambda_i)^{n_{i,j}} \rangle \right).$$

En tant que  $k$ -espace vectoriel<sup>14</sup>,  $M$  est de dimension finie  $n$  et le membre de droite ne l'est que si, et seulement si,  $r = 0$  si bien que

$$k^n \cong_{k[X]\text{-mod.}} \bigoplus_{i=1}^t \bigoplus_{j=1}^{j_i} k[X]/\langle (X - \lambda_i)^{n_{i,j}} \rangle.$$

Notons  $\psi$  cet isomorphisme et pour tout  $i \in \{1, \dots, t\}$  et  $j \in \{1, \dots, j_i\}$ , on note  $\pi_{i,j} : k[X] \rightarrow k[X]/\langle (X - \lambda_i)^{n_{i,j}} \rangle$  la surjection canonique. On sait alors<sup>15</sup> que la famille

$$\mathcal{B}_{i,j} = \left( \pi_{i,j}(1), \dots, \pi_{i,j}\left((X - \lambda_i)^{n_{i,j}-1}\right) \right)$$

est une base du  $k$ -espace vectoriel  $k[X]/\langle (X - \lambda_i)^{n_{i,j}} \rangle$ . On vérifie aisément que la matrice de la multiplication par  $X$  est donnée par  $J_{n_{i,j}}(\lambda_i)$  car pour tout  $s \in \{0, \dots, n_{i,j} - 1\}$ , on a

$$X \cdot \pi_{i,j}((X - \lambda_i)^s) = \pi_{i,j}(X(X - \lambda_i)^s) = \pi_{i,j}((X - \lambda_i)^{s+1}) + \lambda_i \pi_{i,j}((X - \lambda_i)^s).$$

12. Voir page 27.

13. On combine 3.6 et 3.11 des notes de cours.

14. Noter que cet isomorphisme de  $k[X]$ -modules est en particulier un isomorphisme de  $k$ -espace vectoriels.

15. Voir exercice 14.

Il suffit alors de considérer la base

$$\mathcal{B} = \left( \psi^{-1}(\mathcal{B}_{1,1}), \dots, \psi^{-1}(\mathcal{B}_{1,j_1}), \dots, \psi^{-1}(\mathcal{B}_{t,1}), \dots, \psi^{-1}(\mathcal{B}_{t,j_t}) \right)$$

dans laquelle la matrice  $M$  a bien la forme voulue, à savoir

$$\begin{pmatrix} J_{n_{1,1}}(\lambda_1) & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & J_{n_{1,j_1}}(\lambda_1) & & & & & & & \\ & & & \ddots & & & & & & \\ & & & & J_{n_{t,1}}(\lambda_t) & & & & & \\ & & & & & \ddots & & & & \\ & & & & & & & & J_{n_{t,j_t}}(\lambda_t) & \\ & & & & & & & & & \ddots \end{pmatrix}$$

Noter qu'on a unicité à permutation près (qui découle de l'unicité dans le théorème de structure). On a alors que les  $\lambda_j$  sont les valeurs propres de  $M$  et que  $j_j = \dim(\text{Ker}(M - \lambda_j I_n))$  et on voit également que deux matrices sont semblables si, et seulement si, pour tout  $\lambda \in k$ , le nombre de blocs de la forme  $J_r(\lambda)$  apparaissant dans une réduction de Jordan est le même pour les deux matrices. Bien sûr, tout ce qui précède reste valable dans le cas d'un polynôme caractéristique scindé! En effet, par le théorème de structure, on dispose d'un entier  $s$  et de polynômes non constants  $P_1 \mid \dots \mid P_s$  tels que<sup>16</sup>

$$k^n \cong {}_{k[X]}k[X]\text{-mod.} \cong \bigoplus_{i=1}^s k[X]/(P_i).$$

Puisque le produit des  $P_i$  est égale à  $\chi_M$  que l'on suppose scindé, chacun des  $P_i$  est scindé et on peut écrire

$$P_i = \prod_{j=1}^{j_i} (X - \lambda_j)^{n_{i,j}}$$

avec  $n_{i,1} \leq \dots \leq n_{i,j_i}$  et le lemme chinois nous permet de nous ramener à la démonstration ci-dessus. On a également que le nombre d'invariants de similitudes est donné par

$$s = \max\{j_\lambda : \lambda \in k\}.$$

Finalement, le lien entre réduction de Frobenius et réduction de Jordan réside dans le théorème chinois et le passage du théorème de structure au théorème en composantes  $p$ -primaires!

16. En effet, si  $\pi_i : k[X] \rightarrow k[X]/(P_i)$  est la surjection canonique, alors la matrice de la multiplication par  $X$  dans la base  $(\pi_i(1), \dots, \pi_i(X)^{\deg(P_i)-1})$  est la matrice compagnon  $C_{P_i}$  et le théorème des invariants de similitude résulte de l'isomorphisme

$$k^n \cong {}_{k[X]}k[X]\text{-mod.} \cong \bigoplus_{i=1}^s k[X]/(P_i)$$

dans la base  $(\pi_1(1), \dots, \pi_1(X)^{\deg(P_1)-1}, \dots, \pi_s(1), \dots, \pi_s(X)^{\deg(P_s)-1})$ . En réalité, on a même une réciproque. S'il existe une base  $\mathcal{B}$  dans laquelle la matrice d'un endomorphisme d'un  $k$ -espace vectoriel  $E$ , noté  $u$ , est la matrice compagnon  $C_P$ , alors en tant que  $k[X]$ -module, on a

$$(E, u) \cong {}_{k[X]}k[X]\text{-mod.} \cong k[X]/(P).$$

En effet, la structure de  $k[X]$ -module de  $k[X]/(P)$  est précisément celle obtenue à partir du  $k$ -espace vectoriel  $k[X]/(P)$  et de l'endomorphisme donné par la multiplication par  $X$ , dont la matrice dans la base mentionnée précédemment est alors bien  $C_P$ . Cela fournit un isomorphisme puisque pour deux espaces vectoriels  $E$  et  $F$  munis respectivement de deux endomorphismes  $u$  et  $v$ , on a un isomorphisme de  $k[X]$ -modules entre  $(E, u)$  et  $(F, v)$  si, et seulement si,  $u$  et  $v$  sont semblables. Cela s'obtient à partir du fait que cela signifie qu'il existe une application  $k[X]$ -linéaire  $\varphi : E \rightarrow F$ . Cela équivaut à se donner une application  $k$ -linéaire et bijective telle que, pour tout  $x \in E$ , on ait  $\varphi(X \cdot x) = \varphi \circ u(x) = X \cdot \varphi(x) = v \circ \varphi(x)$  soit  $v = \varphi \circ u \circ \varphi^{-1}$ . Mentionnons alors que les sous- $k[X]$ -modules de  $(E, u)$  correspondent aux  $(F, u|_F)$  pour  $F$  un sous-espace vectoriel de  $E$  stable par  $u$ . En effet, si  $N$  est un tel sous-module, en particulier  $N$  est un sous-espace vectoriel de  $E$ . Par ailleurs, pour tout  $n \in N$  et  $P \in k[X]$ , on a  $P \cdot n = P(u)(n) \in N$  donc pour  $P = X$ , on voit que  $N$  est stable par  $u$ . Réciproquement, si on se donne un sous-espace vectoriel stable, alors pour tout  $n \in N$ ,  $X \cdot n \in N$  et on obtient en itérant et par linéarité que pour tout  $P \in k[X]$ , on a  $P \cdot n \in N$  et on a donc bien un sous- $k[X]$ -module.

4. Dans le cas  $k = \mathbf{R}$ , en reprenant un raisonnement analogue, les irréductibles unitaires sont les polynômes de la forme  $X - x$  pour  $x \in k$  et  $X^2 + aX + b$  avec  $a^2 - 4b < 0$ . Les polynômes précédents étant tous 2 à 2 non associés. Un raisonnement analogue à celui de la question précédente garantit que

$$k^n \cong \bigoplus_{i=1}^t \bigoplus_{j=1}^{j_i} k[X]/\langle (X - x_i)^{n_{i,j}} \rangle \oplus \bigoplus_{k=1}^s \bigoplus_{\ell=1}^{\ell_k} k[X]/\langle (X^2 + a_k X + b_k)^{m_{k,\ell}} \rangle \quad \forall k \in \{1, \dots, s\}, \quad a_k^2 < 4b_k.$$

Notant  $\psi$  cet isomorphisme, on a alors que dans la base

$$\left( \psi^{-1}(\mathcal{B}_{1,1}), \dots, \psi^{-1}(\mathcal{B}_{1,j_1}), \dots, \psi^{-1}(\mathcal{B}_{t,1}), \dots, \psi^{-1}(\mathcal{B}_{t,j_t}) \right)$$

la matrice restreinte à

$$\psi^{-1} \left( \bigoplus_{i=1}^t \bigoplus_{j=1}^{j_i} k[X]/\langle (X - x_i)^{n_{i,j}} \rangle \right)$$

est diagonale par blocs de la forme

$$\begin{pmatrix} J_{n_{1,1}}(x_1) & & & & & & \\ & \ddots & & & & & \\ & & J_{n_{1,j_1}}(x_1) & & & & \\ & & & \ddots & & & \\ & & & & J_{n_{t,1}}(x_t) & & \\ & & & & & \ddots & \\ & & & & & & J_{n_{t,j_t}}(x_t) \end{pmatrix}.$$

Maintenant, pour tout  $k \in \{1, \dots, s\}$  et  $\ell \in \{1, \dots, \ell_k\}$ , on note  $\pi_{k,\ell} : k[X] \rightarrow k[X]/\langle (X^2 + a_k X + b_k)^{m_{k,\ell}} \rangle$  la surjection canonique. On a alors que la famille

$$\mathcal{B}'_{k,\ell} = \left( \pi_{k,\ell}(1), \pi_{k,\ell}(X), \pi_{k,\ell}(X^2 + a_k X + b_k), \pi_{k,\ell}(X(X^2 + a_k X + b_k)), \dots, \pi_{k,\ell}(X^2 + a_k X + b_k)^{m_{k,\ell}-1}, \pi_{k,\ell}(X(X^2 + a_k X + b_k))^{m_{k,\ell}-1} \right)$$

est une base du  $k$ -espace vectoriel  $k[X]/\langle (X^2 + a_k X + b_k)^{m_{k,\ell}} \rangle$ . On a bien  $2m_{k,\ell}$  vecteurs dans un espace de dimension  $2m_{k,\ell}$  (voir à nouveau l'exercice 14) et on vérifie aisément que la famille est libre car toute combinaison linéaire de ces vecteurs fournit un polynôme de degré  $< 2m_{k,\ell}$  de classe nulle, autrement dit ce polynôme est nul et on conclut grâce au fait que la famille est échelonnée en degrés. On vérifie ensuite aisément que la matrice de la multiplication par  $X$  est donnée par

$$\begin{pmatrix} 0 & -b_k & 0 & 0 & & \\ 1 & -a_k & 0 & 0 & & \\ 0 & 1 & 0 & -b_k & & \\ 0 & 0 & 1 & -a_k & & \\ 0 & 0 & 0 & 1 & & \\ & & & & \ddots & \end{pmatrix} \in \mathcal{M}_{2m_{k,\ell}}(k). \quad (*)$$

En effet, les colonnes avec uniquement des 0 et un unique 1 sont claires. Pour les autres, on a que

$$\begin{aligned} X \cdot \pi_{k,\ell}(X(X^2 + a_k X + b_k)^p) &= \pi_{k,\ell}(X^2(X^2 + a_k X + b_k)^p) \\ &= \pi_{k,\ell}((X^2 + a_k X + b_k)^{p+1}) - a_k \pi_{k,\ell}(X(X^2 + a_k X + b_k)^p) - b_k \pi_{k,\ell}((X^2 + a_k X + b_k)^p). \end{aligned}$$

Ainsi, dans la base

$$\left( \psi^{-1}(\mathcal{B}_{1,1}), \dots, \psi^{-1}(\mathcal{B}_{1,j_1}), \dots, \psi^{-1}(\mathcal{B}_{t,1}), \dots, \psi^{-1}(\mathcal{B}_{t,j_t}), \mathcal{B}'_{1,1}, \dots, \psi^{-1}(\mathcal{B}'_{1,\ell_1}), \dots, \psi^{-1}(\mathcal{B}'_{s,1}), \dots, \psi^{-1}(\mathcal{B}'_{s,\ell_s}) \right),$$

17. On rappelle que pour un polynôme à coefficients réels irréductible et unitaire de degré supérieur à 2, ce polynôme admet une racine  $\lambda \in \mathbf{C} \setminus \mathbf{R}$ . Il admet alors également  $\bar{\lambda}$  comme racine et est donc divisible par  $(X - \lambda)(X - \bar{\lambda})$  et donc égal à  $(X - \lambda)(X - \bar{\lambda})$ . Autrement dit, il est de la forme ci-après. On rappelle également que le théorème des valeurs intermédiaires fournit une racine réelle pour tout polynôme de degré impair.

notre matrice  $M$  de départ est diagonale par blocs avec des blocs de la forme  $J_n(\lambda)$  suivis de blocs de la forme <sup>18</sup> (\*) avec  $a_k^2 < 4b_k$ .

5. Dans le cas de  $\chi_u = X^4$ , la seule valeur propre est 0 et il suffit de répartir la multiplicité entre les différents blocs  $J_n(0)$ . Or, on a

$$4 = 4 + 0 = 3 + 1 = 2 + 1 + 1 = 2 + 2 = 1 + 1 + 1 + 1$$

qui correspondent respectivement aux réduites de Jordan

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, 0.$$

On remarque que dans ce cas, les réduites de Jordan coïncident avec celles de Frobenius.

Dans le cas  $\chi_u = X(X - 1)(X - 2)(X - 3)$ , on a 4 valeurs propres distinctes et on n'a donc pas le choix, on a une unique réduite de Jordan qui est  $\text{diag}(0, 1, 2, 3)$ .

Enfin, lorsque  $\chi_u = (X^2 + 1)(X^2 + X + 1)^2$ , les valeurs propres sont  $\pm i, j$  et  $j^2$ , de multiplicités respectives 1, 2 et 2. On peut écrire  $2 = 2 + 0 = 1 + 1$  si bien qu'on obtient les quatre réduites de Jordan suivantes <sup>19</sup> :

$$\begin{pmatrix} i & 0 & 0 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 & 0 & 0 \\ 0 & 0 & j & 0 & 0 & 0 \\ 0 & 0 & 1 & j & 0 & 0 \\ 0 & 0 & 0 & 0 & j^2 & 0 \\ 0 & 0 & 0 & 0 & 1 & j^2 \end{pmatrix}, \begin{pmatrix} i & 0 & 0 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 & 0 & 0 \\ 0 & 0 & j & 0 & 0 & 0 \\ 0 & 0 & 1 & j & 0 & 0 \\ 0 & 0 & 0 & 0 & j^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & j^2 \end{pmatrix}, \begin{pmatrix} i & 0 & 0 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 & 0 & 0 \\ 0 & 0 & j & 0 & 0 & 0 \\ 0 & 0 & 0 & j & 0 & 0 \\ 0 & 0 & 0 & 0 & j^2 & 0 \\ 0 & 0 & 0 & 0 & 1 & j^2 \end{pmatrix}, \begin{pmatrix} i & 0 & 0 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 & 0 & 0 \\ 0 & 0 & j & 0 & 0 & 0 \\ 0 & 0 & 0 & j & 0 & 0 \\ 0 & 0 & 0 & 0 & j^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & j^2 \end{pmatrix}.$$

6. (i) On a alors

$$(E, u) \cong k[X]/\langle X(X - 1) \rangle \oplus k[X]/\langle X(X - 1) \rangle$$

et par le théorème chinois

$$(E, u) \cong (k[X]/(X))^2 \oplus (k[X]/(X - 1))^2$$

de sorte que l'on obtient la réduite de Jordan

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

(ii) De même, on a

$$(E, u) \cong k[X]/\langle X^2(X - 1) \rangle \oplus k[X]/\langle X - 1 \rangle \cong k[X]/(X^2) \oplus (k[X]/(X - 1))^2$$

et

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

18. On peut aussi choisir ces blocs de la forme  $K_k$  avec

$$K_k = \begin{pmatrix} \Lambda_k & 0 & 0 & 0 \\ I_2 & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & I_2 & \Lambda_k \end{pmatrix} \text{ avec } \Lambda_k = \begin{pmatrix} x_k & -y_k \\ y_k & x_k \end{pmatrix}.$$

et alors les valeurs propres réelles correspondent aux blocs  $J_n(\lambda)$  et les valeurs propres non réelles sont les  $x_k \pm iy_k$ . Pour démontrer ce résultat, on établit que cette décomposition par blocs et la matrice de départ ont la même réduction de Jordan sur  $\mathbf{C}$  (exercice!).

19. Qui correspondent bien aux 4 réduites de Frobenius de 2, et je vous laisse déterminer laquelle correspond à laquelle!

(iii) De même, on a

$$(E, u) \cong k[X]/\langle X(X-1)^2 \rangle \oplus k[X]/(X) \cong k[X]/\langle (X-1)^2 \rangle \oplus (k[X]/(X))^2$$

et

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

(iv) De même, on a

$$(E, u) \cong k[X]/\langle X^2(X-1)^2 \rangle \cong k[X]/(X^2) \oplus k[X]/\langle (X-1)^2 \rangle$$

et

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

7. C'est la même chose qu'en question précédente mais à l'envers (à rapprocher de l'exercice 1)! On a dans le premier cas à partir de la réduction de Jordan

$$(E, u) \cong k[X]/\langle (X-1)^3 \rangle \oplus k[X]/\langle (X-1)^2 \rangle \oplus k[X]/(X^2) \oplus k[X]/(X).$$

On a vu plus haut que cela implique  $s = 2$ . On considère alors la plus grande puissance de chacun des facteurs irréductibles et on pose  $P_2 = X^2(X-1)^3$  et par le théorème chinois

$$(E, u) \cong k[X]/(P_2) \oplus k[X]/\langle (X-1)^2 \rangle \oplus k[X]/(X).$$

En itérant, il vient de même  $P_1 = X(X-1)^2$  de sorte que

$$(E, u) \cong k[X]/(P_2) \oplus k[X]/(P_1)$$

avec  $P_1 \mid P_2$  et donc il s'agit des invariants de similitudes.

De même, on trouve dans le second cas  $P_2 = (X-1)^2(X-2)^2(X-3)^3$  et  $P_1 = (X-1)(X-2)^2$  et dans le dernier cas  $P_3 = P_2 = (X-1)(X-2)$  et  $P_1 = X-1$ .

8. On utilise alors les informations du Lemme 3.16 des notes de cours. On sait que  $d_1$  le plus petit facteur invariant est le pgcd des mineurs d'ordre 1, autrement dit le pgcd des coefficients de la matrice. On obtient ici que  $d_1 = X-1$ . On a alors que  $d_2$  est le quotient du pgcd des mineurs de taille 2 par  $d_1$ . Les mineurs de taille 2 sont

$$(X+1)(X-1)^2(X^2+X+2), \quad (X+1)(X-1)^2(X+11) \quad \text{et} \quad (X-1)^2(X^3-3X^2+8X-10)$$

de sorte que  $d_2 = (X-1)^2/d_1 = X-1$ .

Enfin, on sait que pour obtenir les invariants de similitude cherchés, il suffit de calculer les facteurs invariants de la matrice  $M - XI_3 \in \mathcal{M}_3(\mathbf{Q}[X])$ . On procède alors comme ci-dessus pour obtenir que  $d_1 = 1$ . Puis le pgcd de tous les mineurs de taille 2 est donné par  $X-1$  si bien que  $d_2 = X-1$  et le polynôme caractéristique de  $M$  est donné par  $(X-1)^3$  si bien que  $d_3 = \frac{(X-1)^3}{d_1 d_2} = (X-1)^2$  et les invariants de similitude de  $M$  sont donc  $P_1 = X-1$  et  $P_2 = (X-1)^2$ .

**REMARQUE :** Dans le cas d'un anneau euclidien  $A$  de stathme  $\varphi$  (comme  $\mathbf{Q}[X]$  avec le degré), nous disposons aussi d'un algorithme utilisant la division euclidienne pour calculer les facteurs invariants d'une matrice  $M \in \mathcal{M}_n(A)$  ainsi que les matrices  $P$  et  $Q$  de changement de bases. L'algorithme (qu'ils était un peu long et fastidieux à mettre en œuvre ici) se trouve p. 286 de l'ouvrage *Objectif Agrégation* de Beck, Malick et Peyré.

**EXERCICE 5.**

1. Soit  $k$  un corps. Montrer que le morphisme naturel de  $k$ -algèbres de  $k(X) \otimes k(Y)$  vers  $k(X, Y)$  est injectif mais non surjectif.

- Soit  $L$  une extension de  $K$ . Montrer que  $K(T) \otimes_K L$  est isomorphe au sous-anneau de  $L(T)$  constitué des  $\frac{P}{Q}$  avec  $P \in L[T]$  et  $Q$  non nul dans  $K[T]$ . Ce sous-anneau est-il un corps ?
- Cette question fait appel à l'exercice 2 de la feuille de TD III. Soient  $A$  un anneau et  $S$  une partie multiplicative de  $A$ . Montrer que l'on a un isomorphisme canonique de  $S^{-1}A$ -modules

$$S^{-1}(M_1 \otimes_A \cdots \otimes_A M_N) \cong S^{-1}M_1 \otimes_{S^{-1}A} \cdots \otimes_{S^{-1}A} S^{-1}M_n.$$

**SOLUTION.**

- On dispose d'une application bilinéaire naturelle  $\varphi : K(X) \times K(Y) \rightarrow K(X, Y)$  définie par  $(P(X), Q(Y)) \mapsto P(X)Q(Y)$  qui induit par conséquent une application linéaire (et en fait un morphisme de  $K$ -algèbres)  $\tilde{\varphi} : K(X) \otimes_K K(Y) \rightarrow K(X, Y)$  définie par  $\tilde{\varphi}(P(X) \otimes Q(Y)) = P(X)Q(Y)$ . On voit que l'image de  $\tilde{\varphi}$  est incluse dans le sous-espace strict

$$V = \{R(X, Y) \in K(X, Y) : \exists(Q_1(X), Q_2(Y)) \in K[X] \setminus \{0\} \times K[Y] \setminus \{0\} \text{ tels que } R(X, Y)Q_1(X)Q_2(Y) \in K[X, Y]\}$$

(qui ne contient par exemple pas  $\frac{1}{X+Y}$ ), ce qui montre que  $\tilde{\varphi}$  n'est pas surjective.

Étudions à présent l'injectivité en considérant le noyau de  $\tilde{\varphi}$ . Un élément de  $K(X) \otimes_K K(Y)$  est de la forme

$$\sum_{i=1}^t \frac{a_i(X)}{b(X)} \otimes \frac{c_i(Y)}{d(Y)}$$

pour des polynômes  $a_i, b \in K[X]$  et  $c_i, d \in K[Y]$  avec  $b$  et  $d$  non nuls (on a ici considéré un dénominateur commun). Puisque d'après le cours, on a une structure de  $K$ -algèbre, il vient que

$$\sum_{i=1}^t \frac{a_i(X)}{b(X)} \otimes \frac{c_i(Y)}{d(Y)} = \left( \frac{1}{b(X)} \otimes \frac{1}{d(Y)} \right) \left( \sum_{i=1}^t a_i(X) \otimes c_i(Y) \right).$$

Un tel élément est dans le noyau de  $\tilde{\varphi}$  si, et seulement si,

$$\frac{\sum_{i=1}^t a_i(X)c_i(Y)}{b(X)d(Y)} = 0 \quad \text{soit} \quad \sum_{i=1}^t a_i(X)c_i(Y) = 0.$$

Cela implique que  $\sum_{i=1}^t a_i(X) \otimes c_i(Y)$  est dans le noyau de l'isomorphisme  $K[X] \otimes_K K[Y] \rightarrow K[X, Y]$  qui est injectif

donc  $\sum_{i=1}^t a_i(X) \otimes c_i(Y) = 0$  et notre élément de départ dans le noyau est nul, ce qui montre bien l'injectivité. On a en réalité que  $K(X) \otimes_K K(Y) \cong V$ . L'isomorphisme est alors donné par

$$\tilde{\psi} : \begin{cases} V & \longrightarrow & K(X) \otimes_K K(Y) \\ \frac{\sum_{n,m} \lambda_{n,m} X^m Y^n}{Q_1(X)Q_2(Y)} & \longmapsto & \sum_{n,m} \lambda_{n,m} \frac{X^m}{Q_1(X)} \otimes \frac{Y^n}{Q_2(Y)} \end{cases}$$

où l'on a  $\tilde{\psi} \circ \tilde{\varphi} = \text{Id}$  car

$$\frac{P(X)}{B(X)} \otimes \frac{Q(Y)}{C(Y)} \longmapsto \frac{P(X)Q(Y)}{B(X)C(Y)} = \sum_{n,m} p_m q_m \frac{X^m}{B(X)} \frac{Y^n}{C(Y)} \longmapsto \sum_{n,m} p_m q_m \frac{X^m}{B(X)} \otimes \frac{Y^n}{C(Y)} = \frac{P(X)}{B(X)} \otimes \frac{Q(Y)}{C(Y)}$$

si  $P = \sum_m p_m X^m$  et  $Q = \sum_n q_n Y^n$  et par linéarité. Cela implique que cette définition ne dépend pas du choix de  $Q_1, Q_2$  et des  $\lambda_{n,m}$  car l'image de la différence des deux est dans le noyau de  $\tilde{\varphi}$ .

20. Si on avait  $Q_1(X)Q_2(Y) = (X+Y)P(X, Y)$ , on aurait alors  $Q_1(X)Q_2(-X) = 0$  et par intégrité  $Q_1 = 0$  ou  $Q_2 = 0$  ce qui est exclu. Noter que comme  $X+Y$  est l'image de  $x \otimes 1 + 1 \otimes y$  et que son inverse n'a pas d'antécédent, cela établit que  $X+Y$  n'est pas inversible dans l'image qui n'est donc pas un corps.

C'est en contraste avec le cas des polynômes vu en cours où un raisonnement analogue fournit que  $k[X] \otimes_k k[Y] \cong k[X, Y]$  envoyant la base  $(X^m \otimes Y^n)_{(m,n) \in \mathbb{N}^2}$  de  $k[X] \otimes_k k[Y]$  sur la base  $(X^m Y^n)_{(m,n) \in \mathbb{N}^2}$  de  $k[X, Y]$ . Autrement dit, cet isomorphisme est donné par

$$\begin{aligned} k[X, Y] &\longrightarrow k[X] \otimes_k k[Y] \\ \sum_{m,n} \lambda_{m,n} X^m Y^n &\longmapsto \sum_{m,n} \lambda_{m,n} X^m \otimes Y^n. \end{aligned}$$

2. La démonstration est parfaitement analogue et on n'obtient pas un corps.
3. On rappelle que  $S^{-1}M$  est défini comme le quotient de  $M \times S$  par la relation d'équivalence  $(x, s) \sim (y, t)$  si, et seulement si il existe  $u \in S$  tel que  $u(xt - ys) = 0$ . On a alors clairement une structure de  $S^{-1}A$  module avec

$$\frac{x}{s} + \frac{x'}{s'} = \frac{xs' + x's}{ss'} \quad \text{et} \quad \frac{a}{s} \cdot \frac{x}{t} = \frac{a \cdot x}{st}.$$

Commençons par établir que  $S^{-1}M \cong S^{-1}A \otimes_A M$  en tant que  $S^{-1}A$ -modules. On considère l'application bilinéaire  $\varphi : S^{-1}A \times M \rightarrow S^{-1}M$  définie par  $(\frac{a}{s}, m) \mapsto \frac{am}{s}$  qui donne lieu à une application linéaire  $f : S^{-1}A \otimes_A M \rightarrow S^{-1}M$ . Cette application est surjective car  $\frac{x}{s} = f\left(\frac{1}{s} \otimes x\right)$ . Montrons alors qu'elle est injective. On voit que

$$f\left(\frac{1}{s} \otimes x\right) = 0 \iff \frac{x}{s} = 0 \iff \exists u \in S \text{ tel que } ux = 0.$$

On a alors si  $f\left(\frac{1}{s} \otimes x\right) = 0$  que  $\frac{1}{s} \otimes x = \frac{u}{us} \otimes x = \frac{1}{us} \otimes ux = 0$ . Maintenant, tout élément de  $S^{-1}A \otimes_A M$  est de la forme (quitte à réduire au même dénominateur)

$$\sum_i \frac{a_i}{s} \otimes x_i = \frac{1}{s} \otimes \left(\sum_i a_i x_i\right)$$

et un élément du noyau est donc nul par ce qui précède et  $f$  est injective, ce qui démontre le résultat.

Par ailleurs, pour deux  $S^{-1}A$ -modules (qui sont donc également des  $A$ -modules)  $M_1$  et  $M_2$ , on a (en tant que  $S^{-1}A$ -modules)

$$M_1 \otimes_A M_2 \cong M_1 \otimes_{S^{-1}A} M_2.$$

On a ici muni  $M_1 \otimes_A M_2$  de la structure de  $S^{-1}A$ -module suivante<sup>21</sup>

$$\frac{a}{s} \cdot (m_1 \otimes m_2) = \left(\frac{am_1}{s}\right) \otimes m_2.$$

En effet, l'application  $S^{-1}A$ -bilinéaire (et donc  $A$ -linéaire)  $M_1 \times M_2 \rightarrow M_1 \otimes_{S^{-1}A} M_2$  donne lieu à une application linéaire  $f_1 : M_1 \otimes_A M_2 \rightarrow M_1 \otimes_{S^{-1}A} M_2$  telle que  $m_1 \otimes_A m_2 \mapsto m_1 \otimes_{S^{-1}A} m_2$ . Réciproquement, considérons l'application  $A$ -bilinéaire canonique  $M_1 \times M_2 \rightarrow M_1 \otimes_A M_2$ . Elle est clairement  $S^{-1}A$ -bilinéaire pour la structure de  $S^{-1}A$ -module définie plus haut et ces deux morphismes sont inverses l'un de l'autre donc des isomorphismes.

On a donc<sup>22</sup>

$$\begin{aligned} S^{-1}M_1 \otimes_{S^{-1}A} S^{-1}M_2 &\cong (S^{-1}A \otimes_A M_1) \otimes_{S^{-1}A} (S^{-1}A \otimes_A M_2) \\ &\cong (S^{-1}A \otimes_A M_1) \otimes_A (S^{-1}A \otimes_A M_2) \cong (M_1 \otimes_A M_2) \otimes_A (S^{-1}A \otimes_A S^{-1}A) \\ &\cong (M_1 \otimes_A M_2) \otimes_A S^{-1}A \cong S^{-1}(M_1 \otimes_A M_2). \end{aligned}$$

21. Noter que la seconde structure naturelle

$$\frac{a}{s} \cdot (m_1 \otimes m_2) = m_1 \otimes \left(\frac{am_2}{s}\right)$$

est équivalente car

$$m_1 \otimes \left(\frac{am_2}{s}\right) = a \left(m_1 \otimes \left(\frac{m_2}{s}\right)\right) = (am_1) \otimes \left(\frac{m_2}{s}\right) = \left(s \frac{am_1}{s}\right) \otimes \left(\frac{m_2}{s}\right) = s \left(\left(\frac{am_1}{s}\right) \otimes \left(\frac{m_2}{s}\right)\right) = \left(\frac{am_1}{s}\right) \otimes m_2.$$

On peut même montrer que c'est l'unique structure de  $S^{-1}A$ -module compatible avec celle de  $A$ -module.

22. On aurait aussi pu utiliser que pour deux  $A$ -modules  $M_1$  et  $M_2$  et  $S$  une  $A$ -algèbre

On a utilisé l'associativité du produit tensoriel et le fait que

$$S^{-1}A \otimes_A S^{-1}A \cong S^{-1}A.$$

On a une application bilinéaire  $S^{-1}A \times S^{-1}A \rightarrow S^{-1}A$  donnée par  $\left(\frac{a}{s}, \frac{a'}{s'}\right) \mapsto \frac{aa'}{ss'}$  qui donne une application linéaire  $f : S^{-1}A \otimes_A S^{-1}A \rightarrow S^{-1}A$ . Cette application est surjective car  $\frac{a}{s} = f\left(\frac{1}{s} \otimes a\right)$  et injective comme ci-dessus<sup>23</sup>. On conclut par récurrence.

**EXERCICE 6.**

1. Soient  $A$  un anneau commutatif,  $M$  et  $M'$  deux  $A$ -modules et  $S$  une  $A$ -algèbre. Montrer qu'on a un morphisme naturel de  $S$ -modules  $\text{Hom}_A(M, M') \otimes_A S \rightarrow \text{Hom}_S(M \otimes_A S, M' \otimes_A S)$  et qu'il s'agit d'un isomorphisme dans le cas où  $M$  et  $M'$  sont libres de type fini.
2. Soient  $A$  un anneau commutatif et  $S_1, S_2$  deux  $A$ -algèbres. On considère  $\iota_1 : S_1 \rightarrow S_1 \otimes_A S_2$  définie par  $\iota_1(s_1) = s_1 \otimes 1$  et  $\iota_2 : S_2 \rightarrow S_1 \otimes_A S_2$  définie par  $\iota_2(s_2) = 1 \otimes s_2$ . Montrer que  $\iota_1|_A = \iota_2|_A$  et que  $\iota_1(s_1)$  commute avec  $\iota_2(s_2)$  pour tous  $(s_1, s_2) \in S_1 \times S_2$ . Enfin, établir que  $\iota_i$  est injective si  $S_i$  est libre en tant que  $A$ -module pour  $i \in \{1, 2\}$  ou si  $A$  est un corps. Que dire du cas général?
3. Avec les notations de la question précédente, , montrer que pour tout  $A$ -algèbre  $C$  et tout morphismes de  $A$ -algèbres  $\varphi_i : S_i \rightarrow C$  pour  $i \in \{1, 2\}$  tels que  $\varphi_1(s_1)$  commute avec  $\varphi_2(s_2)$  pour tous  $(s_1, s_2) \in S_1 \times S_2$ , il existe un unique morphisme de  $A$ -algèbres  $\chi : S_1 \otimes_A S_2 \rightarrow C$  tel que  $\chi \circ \iota_i = \varphi_i$  pour  $i \in \{1, 2\}$  et envoyant  $s_1 \otimes s_2$  sur  $\varphi_1(s_1)\varphi_2(s_2)$ .
4. En déduire de deux façons différentes que si  $n \in \mathbf{N}^\times$ , pour tout anneau commutatif  $A$  et toute  $A$ -algèbre  $R$ , on a un isomorphisme de  $A$ -algèbres  $\mathcal{M}_n(A) \otimes_A R \cong \mathcal{M}_n(R)$ .

**SOLUTION.**

1. Pour tout  $\varphi \in \text{Hom}_A(M, M')$ , on peut considérer l'application  $A$ -linéaire définie par  $1 \otimes \varphi : M \otimes_A S \rightarrow M' \otimes_A S$  définie par  $m \otimes s \mapsto \varphi(m) \otimes s$ . C'est en réalité une application  $S$ -linéaire car

$$(1 \otimes \varphi)(s'(m \otimes s)) = (1 \otimes \varphi)(m \otimes (s's)) = \varphi(m) \otimes (s's) = s'(\varphi(m) \otimes s) = s'(1 \otimes \varphi)(m \otimes s).$$

On définit alors une application bilinéaire  $\text{Hom}_A(M, M') \times S \cong \text{Hom}_S(M \otimes_A S, M' \otimes_A S)$  par<sup>24</sup>  $(\varphi, s) \mapsto s(1 \otimes \varphi)$  qui fournit donc une unique application  $A$ -linéaire  $L : \text{Hom}_A(M, M') \otimes_A S \cong \text{Hom}_S(M \otimes_A S, M' \otimes_A S)$  telle que  $L(\varphi \otimes s) = s\varphi_S$  où l'on notera  $\varphi_S = 1 \otimes \varphi$  pour éviter les confusions entre l'application  $1 \otimes \varphi$  et le tenseur pur  $\varphi \otimes 1 \in \text{Hom}_A(M, M') \otimes_A S$ . Cette application est  $S$ -linéaire car

$$L(s'(\varphi \otimes s)) = L(\varphi \otimes (s's)) = (s's)\varphi_S = s'L(\varphi \otimes s)$$

et est en réalité un morphisme de  $S$ -algèbre dans le cas où  $M = M'$  car<sup>25</sup> on a alors

$$L((\varphi \otimes s)(\psi \otimes s')) = L((\varphi \circ \psi) \otimes (ss')) = (ss')(\varphi \circ \psi)_S.$$

On vérifie alors que

$$(\varphi \circ \psi)_S(m \otimes s) = \varphi(\psi(m)) \otimes s = \varphi_S(\psi(m) \otimes s) = \varphi_S \circ \psi_S(m \otimes s)$$

23. Que l'on pourrait directement appliquer avec  $M = S^{-1}A$ .

24. Où  $s(1 \otimes \varphi)$  est l'application  $S$ -linéaire  $M \otimes_A S \rightarrow M' \otimes_A S$  donnée par  $m \otimes s' \mapsto \varphi(m) \otimes (ss')$ .

25. En effet, on a bien deux  $S$ -algèbres et

$$\begin{aligned} L\left(\left(\sum_i m_i \otimes s_i\right) \cdot \left(\sum_j n_j \otimes s'_j\right)\right) &= L\left(\sum_{i,j} (m_i \otimes s_i)(n_j \otimes s'_j)\right) = \sum_{i,j} L((m_i \otimes s_i)(n_j \otimes s'_j)) = \sum_{i,j} L(m_i \otimes s_i)L(n_j \otimes s'_j) \\ &= \left(\sum_i L(m_i \otimes s_i)\right) \cdot \left(\sum_j L(n_j \otimes s'_j)\right) \\ &= L\left(\sum_i m_i \otimes s_i\right) \cdot L\left(\sum_j n_j \otimes s'_j\right). \end{aligned}$$



si bien que  $L((\varphi \otimes s)(\psi \otimes s')) = (s\varphi_S) \circ (s'\psi_S) = L(\varphi \otimes s) \circ L(\psi \otimes s')$ . Si maintenant  $M$  et  $M'$  sont libres de type fini. Si les deux modules sont nuls, c'est clair et sinon on choisit  $(e_i)$  et  $(e'_i)$  des bases respectives. On sait alors que des  $S$ -bases de  $M \otimes_A S$  et de  $M' \otimes_A S$  sont  $(e_i \otimes 1)$  et  $(e'_i \otimes 1)$  tandis qu'une  $A$ -base de  $\text{Hom}_A(M, M')$  est donnée par les fonctions  $\varphi_{ij}$  envoyant  $e_i$  sur  $e'_j$  et tous les autres vecteurs  $e_k$  sur 0 et une  $S$ -base de  $\text{Hom}_A(M, M') \otimes_A S$  par les  $(\varphi_{ij} \otimes 1)$ . On a de même une base de  $\text{Hom}_S(M \otimes_A S, M' \otimes_A S)$ . On a alors

$$L(\varphi_{ij} \otimes 1)(1 \otimes e_i) = \varphi_{ij}(e_i) \otimes 1 = e'_j \otimes 1$$

tandis que de même  $L(\varphi_{ij} \otimes 1)(1 \otimes e_k) = 0$  pour  $k \neq i$  et  $L$  envoie une base sur une base et est par conséquent un isomorphisme<sup>26</sup>.

Noter qu'en général, on n'obtient pas un isomorphisme. En effet, soit  $A = M' = \mathbf{Z}/p^2\mathbf{Z}$ . On pose alors  $S = M = \mathbf{Z}/p\mathbf{Z}$  où la structure de  $A$ -module est donnée par la réduction modulo  $p$ :  $\pi : A \rightarrow \mathbf{Z}/p\mathbf{Z}$  et pour tout  $x \in A, y \in \mathbf{Z}/p\mathbf{Z}, y \cdot x = \pi(y)x$ . On a alors que tout élément de  $\text{Hom}_A(M, M')$  est déterminé par le choix de  $\varphi(1)$  et puisque  $\varphi((p+1) \cdot 1) = \varphi(1) = (p+1)\varphi(1)$ , on voit qu'il faut que  $\varphi(1) \in p\mathbf{Z}/p^2\mathbf{Z}$  et que cette condition suffit à définir un unique morphisme. On a donc que l'image de l'application linéaire construite est donnée par l'application  $\varphi \otimes s \mapsto [m \otimes s' \mapsto \varphi(m) \otimes (ss')]$ . Mais par  $A$ -linéarité, il vient

$$\varphi(m) \otimes (ss') = (mss')(\varphi(1) \otimes 1) = (pms's')(k \otimes 1) = 0$$

si  $\varphi(1) = pk$  car  $pms's' = 0$  dans  $S$ . En revanche, on a vu que  $\text{Hom}_A(M, M') \cong \mathbf{Z}/p\mathbf{Z}$  et on a en utilisant le fait que  $A/I \otimes_A M = M/IM$  que  $M \otimes_A S \cong \mathbf{Z}/p\mathbf{Z}$  car  $\mathbf{Z}/p\mathbf{Z} = A/(p)$ . On a donc  $\text{Hom}_S(M \otimes_A S, M' \otimes_A S) \cong \text{Hom}_{\mathbf{Z}/p\mathbf{Z}}(\mathbf{Z}/p\mathbf{Z}, \mathbf{Z}/p\mathbf{Z}) \cong \mathbf{Z}/p\mathbf{Z}$ .

2. On a clairement que pour tout  $a \in A, A \otimes 1 = a(1 \otimes 1) = 1 \otimes a$  donc  $\iota_{1|_A} = \iota_{2|_A}$ . Par ailleurs, pour tous  $(s_1, s_2) \in S_1 \times S_2$ , on a

$$\iota_1(s_1) \cdot \iota_2(s_2) = (s_1 \otimes 1) \cdot (1 \otimes s_2) = s_1 \otimes s_2 = (1 \otimes s_2) \cdot (s_1 \otimes 1) = \iota_2(s_2) \cdot \iota_1(s_1).$$

Le cas où  $A$  est un corps fournit immédiatement que  $S_1$  et  $S_2$  sont libres et donc l'injectivité de  $\iota_1$  et de  $\iota_2$ . Supposons que  $S_1$  est libre, donc  $S_1 = \bigoplus_{i \in I} A$  et ainsi

$$S_1 \otimes_A S_2 \cong \bigoplus_{i \in I} A \otimes_A S_2 \cong \bigoplus_{i \in I} S_2.$$

On peut alors identifier  $\iota_1$  avec l'application  $S_1 \rightarrow \bigoplus_{i \in I} S_2$  donnée par

$$\sum_{i \in I} \lambda_i e_i \mapsto (\lambda_i)_{i \in I}$$

pour<sup>27</sup>  $(e_i)_{i \in I}$  une base de  $S_1$  en tant que  $A$ -module, ce qui fournit immédiatement l'injectivité. On n'a pas injectivité en général, par exemple prendre  $A = \mathbf{Z}$  et  $S_1$  le  $A$ -module correspondant à un groupe abélien d'ordre 3 engendré par  $g$  et  $S_2 = \mathbf{F}_2$ . On a alors  $2 \cdot g = g^2 \neq 0$  mais

$$\iota_1(2g) = (2g) \otimes 1 = g \otimes 2 = 0.$$

3. Si  $\chi$  existe, alors  $\chi(s_1 \otimes s_2) = \chi(\iota_1(s_1)\iota_2(s_2)) = \varphi_1(s_1)\varphi_2(s_2)$  et  $\chi$  est donc unique.

Reste à construire  $\chi$ . Pour cela, on montre que l'application bilinéaire  $(s_1, s_2) \mapsto \varphi_1(s_1)\varphi_2(s_2)$  donne lieu à un unique morphisme  $\chi$  qui convient.

26. Ce résultat signifie que toute application  $S$ -linéaire après extension de la base provient (à combinaison linéaire près) d'applications linéaires après extension de base mais **PAS** que toute telle application linéaire est l'extension de base d'une application linéaire, ce qui reviendrait à demander que tout élément du produit tensoriel soit un tenseur pur. Noter que la matrice de  $\varphi_S$  est la même que celle de  $\varphi$  dans les bases considérées. Dans le cas général, avec  $A = \mathbf{Z}/p^2\mathbf{Z}, p$  un nombre premier et  $S = M = \mathbf{F}_p$  que l'on voit comme un  $A$ -module grâce à la réduction modulo  $p, A \rightarrow S$ . Notre application  $S$ -linéaire  $\text{Hom}_A(M, A) \otimes_A S \rightarrow \text{Hom}_S(M \otimes_A S, S)$  est d'image nulle. En effet,  $\varphi \otimes s$  est envoyé sur  $s\varphi_S$

27. Noter que  $S_1 \cong \bigoplus_{i \in I} A$  est donné par

$$\sum_{i \in I} \lambda_i e_i \mapsto (\lambda_i)_{i \in I}$$

et que  $(\bigoplus_{i \in I} A) \otimes S_2 \cong \bigoplus_{i \in I} S_2$  est donné par

$$((\lambda_i)_{i \in I}) \otimes b = (\lambda_i b)_{i \in I}.$$

4. Il suffit de prendre  $M = M' = A^n$  dans **1.**, l'application étant donnée par  $M \otimes r = r \cdot M$ .

Pour la seconde méthode, on pose le morphisme  $\varphi_1 : R \rightarrow \mathcal{M}_n(R)$  donné par  $r \mapsto rI_n$  et l'inclusion  $\varphi_2 : \mathcal{M}_n(A) \rightarrow \mathcal{M}_n(R)$  et on applique **2.** pour obtenir un morphisme  $\chi : \mathcal{M}_n(A) \otimes_A R \rightarrow \mathcal{M}_n(R)$ . Il est clair que  $\chi$  est surjective. En effet, soit  $E_{ij}$  une matrice élémentaire, alors pour tout  $r \in R$ ,  $rE_{ij} = \varphi_1(r)\varphi_2(E_{ij}) = \chi(r \otimes E_{ij})$ . Pour l'injectivité, il est souvent plus simple de construire un inverse à gauche de  $\chi$  en travaillant avec les produits tensoriels. Pour cela, il suffit de considérer  $\tilde{\chi} : \mathcal{M}_n(R) \rightarrow \mathcal{M}_n(A) \otimes_A R$  donnée par

$$(m_{ij}) \mapsto \sum_{i,j} E_{ij} \otimes m_{ij}.$$

**EXERCICE 7.**

1. Soit  $A$  un anneau intègre de corps de fractions  $k$  et  $V$  un  $k$ -espace vectoriel. Montrer que  $k \otimes_A V \cong V$  en tant que  $A$ -modules.
2. Calculer les produits tensoriels suivants :  $\mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{R}$  en tant que  $\mathbf{Z}$ -module puis

$$\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C}, \quad \mathbf{Q}(\sqrt{2}) \otimes_{\mathbf{Q}} \mathbf{Q}(\sqrt{3}), \quad (\mathbf{Z}/5\mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{Z}[i].$$

**SOLUTION.**

Attention ici à toujours bien préciser pour quelle structure vous avez un isomorphisme. Par exemple,  $\mathbf{R} \otimes_{\mathbf{Q}} \mathbf{R} \cong \mathbf{R}$  en tant que  $\mathbf{Q}$ -espace vectoriels. En effet, si  $(e_i)_{i \in I}$  est une  $\mathbf{Q}$ -base de  $\mathbf{R}$  alors  $I$  est en bijection<sup>28</sup> avec  $\mathbf{R}$  et  $(e_i \otimes e_j)$  est une base de  $\mathbf{R} \otimes_{\mathbf{Q}} \mathbf{R}$  indexée par  $I \times I$  qui est aussi en bijection avec  $\mathbf{R}$  si bien qu'on a l'isomorphisme annoncé  $\mathbf{R} \otimes_{\mathbf{Q}} \mathbf{R} \cong \mathbf{R}$ . En revanche, en tant que  $\mathbf{R}$ -espace vectoriels,  $\dim_{\mathbf{R}}(\mathbf{R}) = 1$  mais  $\mathbf{R} \otimes_{\mathbf{Q}} \mathbf{R}$  est de dimension infinie<sup>29</sup> (pour la structure provenant de la multiplication sur le facteur de gauche). Par ailleurs,  $\mathbf{R}$  n'a pas de diviseur de 0 tandis que dans  $\mathbf{R} \otimes_{\mathbf{Q}} \mathbf{R}$

$$(\sqrt{2} \otimes 1 + 1 \otimes \sqrt{2})(\sqrt{2} \otimes 1 - 1 \otimes \sqrt{2}) = 2 \otimes 1 - 1 \otimes 2 = 0$$

mais  $\sqrt{2} \otimes 1 + 1 \otimes \sqrt{2} \neq 0 \neq \sqrt{2} \otimes 1 - 1 \otimes \sqrt{2}$ .

1. Noter qu'en particulier,  $k \otimes_A k \cong k$ . On déduit de l'application  $A$ -bilinéaire  $(x, v) \mapsto xv$  une application linéaire  $f : k \otimes_A V \rightarrow V$ . Elle est surjective car  $v = f(1 \otimes v)$  et injective car  $f(x \otimes v) = xv = 0$  implique  $x = 0$  ou  $v = 0$  soit  $x \otimes v = 0$ . Et si maintenant on considère un élément du noyau, il est de la forme

$$\sum_i \frac{a_i}{s} \otimes v_i = \frac{1}{s} \otimes \left( \sum_i a_i v_i \right)$$

et on conclut comme dans l'exercice 5 qu'on a un isomorphisme de  $A$ -modules. On obtient en réalité un morphisme de  $A$ -algèbre.

2. On en déduit immédiatement que  $\mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{R} \cong \mathbf{R}$  en tant que  $\mathbf{Z}$ -modules<sup>30</sup>. On a alors d'après le cours<sup>31</sup>

$$\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C} \cong \mathbf{C} \otimes_{\mathbf{R}} \mathbf{R}[X]/(X^2 + 1) \cong \mathbf{C}[X]/(X^2 + 1) \cong \mathbf{C}[X]/(X - i) \times \mathbf{C}[X]/(X + i) \cong \mathbf{C} \times \mathbf{C}$$

en tant que  $\mathbf{C}$ -espace vectoriel<sup>32</sup> et même en tant que  $\mathbf{C}$ -algèbres. De même, il vient

$$\mathbf{Q}(\sqrt{2}) \otimes_{\mathbf{Q}} \mathbf{Q}(\sqrt{3}) \cong \mathbf{Q}(\sqrt{2}) \otimes_{\mathbf{Q}} \mathbf{Q}[X]/(X^2 - 3) \cong \mathbf{Q}(\sqrt{2})[X]/(X^2 - 3)$$

qui est un corps car  $X^2 - 3$  est irréductible sur  $\mathbf{Q}(\sqrt{2})[X]$  en tant que  $\mathbf{Q}(\sqrt{2})$ -algèbre. Enfin,

$$(\mathbf{Z}/5\mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{Z}[i] \cong (\mathbf{Z}/5\mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{Z}[X]/(X^2 + 1) \cong (\mathbf{Z}/5\mathbf{Z})[X]/(X^2 + 1) \cong (\mathbf{Z}/5\mathbf{Z})^2$$

car  $X^2 + 1 = (X - 2)(X - 3)$  sur  $\mathbf{Z}/5\mathbf{Z}$  en tant que  $\mathbf{F}_5$ -espace vectoriel.

28. Pour voir cela, il suffit de construire une famille libre indexée par un ensemble en bijection avec  $\mathbf{R}$  et pour cela je vous renvoie à <https://math.stackexchange.com/questions/6244/is-there-a-quick-proof-as-to-why-the-vector-space-of-mathbb-r-over-mathbb>

29. En effet, il n'est pas difficile de voir que si  $M$  est un  $A$ -module libre de base  $(e_i)$ , alors pour toute  $A$ -algèbre  $S$ , le  $S$ -module  $M \otimes_A S$  est libre de base  $(e_i \otimes 1)$ .

30. Vous pouvez montrer de manière analogue que si  $M$  est un  $A$ -module contenu dans  $k$  et  $V$  un  $k$ -espace vectoriel, alors  $M \otimes_A V \cong V$  en tant que  $A$ -module. Par exemple, on peut montrer que  $A = \mathbf{Z}[\sqrt{10}]$  a pour corps de fractions  $k = \mathbf{Q}[\sqrt{10}]$  et que l'idéal  $I = (2, \sqrt{10})$  de  $A$  n'est pas principal. Ainsi,  $I \not\cong A$  en tant que  $A$ -module mais  $I \otimes_A k \cong A \otimes_A k$  en tant que  $A$ -modules.

31. On a vu une description différente dans l'exercice 3.

32. Attention que  $z \otimes w \mapsto (z, w)$  ne fournit pas un isomorphisme car  $(-z) \otimes (-w) = z \otimes w$  mais  $(z, w) \neq (-z, -w)$ .

Cela fait intervenir la notion de deux extensions *linéairement disjointes* qui réapparaîtra et aura des conséquences en théorie de Galois.

**EXERCICE 8.** Soient  $M, M', N, N'$  des  $A$ -modules libres de type fini et  $\varphi : M \rightarrow M'$  et  $\psi : N \rightarrow N'$  deux applications  $A$ -linéaires. On se propose d'étudier quelques propriétés de l'application linéaire  $\varphi \otimes \psi : M \otimes_A M' \rightarrow N \otimes_A N'$ .

1. Décrire la matrice de  $\varphi \otimes \psi$  dans des bases adaptées. La comparer avec celle de  $\psi \otimes \varphi$ .
2. On suppose que  $\text{rang}(M) = \text{rang}(M')$  et que  $\text{rang}(N) = \text{rang}(N')$ . Calculer les valeurs propres de  $\varphi \otimes \psi$  et de  $\varphi \otimes \text{Id} + \text{Id} \otimes \psi$ . Calculer  $\det(\varphi \otimes \psi)$ .
3. Montrer qu'on a un isomorphisme

$$\text{Hom}_A(M, M') \otimes_A \text{Hom}_A(N, N') \longrightarrow \text{Hom}_A(M \otimes_A N, M' \otimes_A N').$$

Que se passe-t-il si l'on supprime les hypothèse de liberté et de type fini ?

4. Soient maintenant  $M'', N''$  deux  $A$ -modules et  $\varphi' : M' \rightarrow M''$  et  $\psi' : N' \rightarrow N''$  deux morphismes. Établir que

$$(\varphi' \otimes \psi') \circ (\varphi \otimes \psi) = (\varphi' \circ \varphi) \otimes (\psi' \circ \psi)$$

dans  $\text{Hom}_A(M \otimes_A N, M'' \otimes_A N'')$ .

5. Montrer que si  $\varphi$  et  $\psi$  sont des isomorphismes, alors  $\varphi \otimes \psi$  aussi. On précisera sa réciproque.
6. Montrer que si  $\varphi$  et  $\psi$  sont surjectives, alors  $\varphi \otimes \psi$  aussi. Le résultat vaut-il pour l'injectivité ?  
*Indication : Considérer  $\alpha : \mathbf{Z}/p\mathbf{Z} \rightarrow \mathbf{Z}/p^2\mathbf{Z}$  donnée par  $x \mapsto px$ .*
7. Si  $\varphi$  est injective et que  $\varphi(M)$  est un facteur direct de  $N$ , alors montrer que pour tout  $k \in \mathbf{N}^\times$ ,  $\varphi^{\otimes k} : M^{\otimes k} \rightarrow N^{\otimes k}$  est injective, d'image un facteur direct de  $N^{\otimes k}$ .
8. Si  $\varphi$  et  $\psi$  sont surjective, établir que  $\text{Ker}(\varphi \otimes \psi)$  est le sous-module de  $M \otimes_A N$  engendré par les  $m \otimes n$  avec  $m \in \text{Ker}(\varphi)$  et  $n \in \text{Ker}(\psi)$ .

**SOLUTION.**

1. Notons  $e_1, \dots, e_n, e'_1, \dots, e'_m, f_1, \dots, f_r$  et  $f'_1, \dots, f'_s$  des bases respectivement de  $M, M', N$  et  $N'$ . On sait alors que  $(e_i \otimes e'_j)$  est une base de  $M \otimes_A M'$  et que  $(f_i \otimes f'_j)$  est une base de  $N \otimes_A N'$ . Notons  $B$  la matrice de  $\varphi$  et  $C$  celle de  $\psi$ . On calcule alors

$$\varphi \otimes \psi(e_i \otimes e'_j) = \varphi(e_i) \otimes \psi(e'_j) = \sum_{k=1}^r \sum_{\ell=1}^s b_{ki} c_{\ell j} f_k \otimes f'_\ell$$

si bien que dans les bases  $(e_1 \otimes e'_1, \dots, e_1 \otimes e'_m, \dots, e_n \otimes e'_1, \dots, e_n \otimes e'_m)$  et  $(f_1 \otimes f'_1, \dots, f_1 \otimes f'_s, \dots, f_r \otimes f'_1, \dots, f_r \otimes f'_s)$ , il vient que la matrice cherchée est donnée par<sup>33</sup>

$$B \otimes C = \begin{pmatrix} b_{11}C & \cdots & b_{1n}C \\ \vdots & \vdots & \vdots \\ b_{r1}C & \cdots & b_{rn}C \end{pmatrix} \in \mathcal{M}_{nm,rs}(A).$$

Cette matrice est appelée le *produit de Kronecker* de  $B$  et  $C$  et on voit facilement qu'en général,  $B \otimes C \neq C \otimes B$ .

2. On vérifie aisément que si  $\lambda$  est valeur propre de  $B$  et  $\mu$  valeur propre de  $C$  avec  $BX = \lambda X$  et  $CY = \mu Y$  où  $X, Y \neq 0$ . On considère alors le vecteur  $X \otimes Y$  défini par  $(x_1 \otimes y_1, \dots, x_1 \otimes y_n, \dots, x_n \otimes y_1, \dots, x_n \otimes y_n)$  est non nul<sup>34</sup> et on vérifie que

$$(B \otimes C)(X \otimes Y) = \lambda\mu X \otimes Y \quad \text{et} \quad (B \otimes I_r + I_n \otimes C)(X \otimes Y) = (\lambda + \mu)X \otimes Y.$$

On peut alors mettre  $B$  et  $C$  sous leur forme de Jordan via  $P$  et  $Q$  (sur une clôture algébrique) et on vérifie que  $P \otimes Q$  triangularise  $B \otimes C$  avec sur la diagonale tous les produits possibles  $\lambda\mu$  et de même pour la somme avec toutes les sommes possibles  $\lambda + \mu$ . On en déduit immédiatement que

$$\text{Tr}(B \otimes C) = \text{Tr}(B)\text{Tr}(C) \quad \text{et} \quad \det(B \otimes C) = \det(B)^n \det(C)^r.$$

33. Traiter des exemples de petite dimension pour s'en convaincre!

34. En effet, si  $M$  et  $N$  sont deux modules libres sur un anneau intègre, alors si  $m \neq 0 \neq n$ , on a  $m \otimes n \neq 0$ . Il suffit pour le voir d'écrire  $m$  et  $n$  dans une base et de développer par bilinéarité.

3. On écrira  $\varphi \otimes_A \psi$  pour désigner le tenseur pur dans  $\text{Hom}_A(M, M') \otimes_A \text{Hom}_A(N, N')$  et éviter les confusions avec l'application linéaire  $\varphi \otimes \psi$ . Comme d'habitude, on part de l'application bilinéaire  $(\varphi, \psi) \mapsto \varphi \otimes \psi$  qui donne lieu à une application  $A$ -linéaire

$$f : \text{Hom}_A(M, M') \otimes_A \text{Hom}_A(N, N') \longrightarrow \text{Hom}_A(M \otimes_A N, M' \otimes_A N')$$

définie par  $f(\varphi \otimes_A \psi) = \varphi \otimes \psi$ . Si l'on suppose que les modules sont libres de type fini, on en considère des bases et on vérifie que l'application envoie une base sur une base comme en 1. En effet, avec les mêmes notations, on sait que  $\text{Hom}_A(M, M')$  et  $\text{Hom}_A(N, N')$  sont libres de bases respectives  $(\varphi_{ij})$  qui envoie  $e_i$  sur  $e'_j$  et tous les autres  $e_k$  sur 0 et  $(\psi_{ij})$  qui envoie  $f_i$  sur  $f'_j$  et tous les autres  $f_k$  sur 0 si bien que  $\text{Hom}_A(M, M') \otimes_A \text{Hom}_A(N, N')$  est libre de base  $(\varphi_{ij} \otimes \psi_{k\ell})$  et de même une base de  $\text{Hom}_A(M \otimes_A N, M' \otimes_A N')$  est donnée par les  $(\theta_{ijk\ell})$  qui envoie  $e_i \otimes f_j$  sur  $e'_k \otimes e'_\ell$  et les autres  $e_t \otimes f_h$  sur 0. On vérifie alors que

$$\begin{aligned} f(\varphi_{ij} \otimes \psi_{k\ell})(e_t \otimes f_h) &= \varphi_{ij}(e_t) \otimes \psi_{k\ell}(f_h) \\ &= \delta_{it} \delta_{hk} (e'_j \otimes f'_\ell) \\ &= \begin{cases} e'_j \otimes f'_\ell & \text{si } i = t \text{ et } h = k \\ 0 & \text{sinon.} \end{cases} \end{aligned}$$

Autrement dit,  $f$  envoie une base sur une base et est donc un isomorphisme.

Sans l'hypothèse libre de type fini, le résultat tombe en défaut. On peut à cette fin considérer  $A = \mathbf{Z}$  et  $M = M' = N = \mathbf{Z}/p\mathbf{Z}$ ,  $N' = \mathbf{Z}/p^2\mathbf{Z}$  et utiliser le fait que l'application  $\alpha : \mathbf{Z}/p\mathbf{Z} \rightarrow \mathbf{Z}/p^2\mathbf{Z}$  défini par  $x \mapsto px$ . On a alors que  $f(\text{Id} \otimes \alpha)$  est donnée par

$$f(\text{Id} \otimes \alpha) : \begin{cases} \mathbf{Z}/p\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/p\mathbf{Z} & \longrightarrow & \mathbf{Z}/p\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/p^2\mathbf{Z} \\ a \otimes x & \longmapsto & a \otimes \alpha(x) = a \otimes (px). \end{cases}$$

Or, on a par  $\mathbf{Z}$ -bilinéarité, que  $a \otimes (px) = (pa) \otimes x = 0$  si bien que  $f(\text{Id} \otimes \alpha) = 0$  mais  $\text{Id} \otimes \alpha \neq 0$  dans  $\text{Hom}_A(M, M') \otimes_A \text{Hom}_A(N, N')$ . En effet,  $\text{Hom}_A(M, M') \cong \mathbf{Z}/p\mathbf{Z}$  et à travers cet isomorphisme<sup>35</sup>, on peut identifier  $\text{Id}$  à 1 tandis que de même à travers l'isomorphisme<sup>36</sup>  $\text{Hom}_A(N, N') \cong \mathbf{Z}/p\mathbf{Z}$  que  $\alpha$  peut s'identifier à 1 si bien qu'on a affaire à  $1 \otimes 1$  dans  $\mathbf{Z}/p\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/p\mathbf{Z}$  qui est non nul car par exemple l'application bilinéaire  $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} \rightarrow \mathbf{Z}/p\mathbf{Z}$  qui envoie  $(\bar{k}, \bar{\ell}) \mapsto \overline{k\ell}$  est non nulle en  $(1, 1)$ . On a donc cependant<sup>37</sup>  $\text{Hom}_A(M, M') \cong \mathbf{Z}/p\mathbf{Z}$  et  $\text{Hom}_A(N, N') \cong \mathbf{Z}/p\mathbf{Z}$  de sorte que  $\text{Hom}_A(M, M') \otimes_A \text{Hom}_A(N, N') \cong \mathbf{Z}/p\mathbf{Z}$  tandis que

$$\text{Hom}_A(M \otimes_A N, M' \otimes_A N') = \text{Hom}_A(\mathbf{Z}/p\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/p\mathbf{Z}, \mathbf{Z}/p\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/p^2\mathbf{Z}) \cong \text{Hom}_A(\mathbf{Z}/p\mathbf{Z}, \mathbf{Z}/p\mathbf{Z}) \cong \mathbf{Z}/p\mathbf{Z}.$$

Noter qu'ici on a fait appel au résultat de la question 5. et que dans le cas de deux isomorphismes  $\varphi_1 : M_1 \cong M_2$  et  $\varphi_2 : N_1 \cong N_2$ , alors on a  $M_1 \otimes_A N_1 \cong M_2 \otimes_A N_2$  via  $\varphi_1 \otimes \varphi_2$ . C'est lorsqu'on a uniquement injectivité que cela peut poser problème comme vous l'avez vu en cours.

4. Il suffit par linéarité de le vérifier sur les tenseurs purs, ce qui est immédiat, la valeur commune en  $m \otimes n$  étant  $\varphi' \circ \varphi(m) \otimes \psi' \circ \psi(n)$ . On a alors  $\text{Id}_M \otimes \text{Id}_N = \text{Id}_{M \otimes_A N}$ .
5. On utilise la question précédente et on vérifie que  $\varphi^{-1} \otimes \psi^{-1}$  est l'inverse.
6. Il suffit de montrer que tout tenseur pur  $m' \otimes n'$  est dans l'image par linéarité et le fait que ces tenseurs purs engendrent  $M' \otimes_A N'$ . Par surjectivité de  $\varphi$  et  $\psi$ , il vient  $m \in M$  et  $n \in N$  tels que  $m' = \varphi(m)$  et  $n' = \psi(n)$  si bien que  $m' \otimes n' = \varphi(m) \otimes \psi(n) = \varphi \otimes \psi(m \otimes n)$ .

Pour l'injectivité, la réponse est non. On l'a vu en question 3. L'application  $\text{Id} \otimes \alpha$  est identiquement nulle sur  $\mathbf{Z}/p\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/p\mathbf{Z} \neq \{0\}$  donc non injective alors que l'identité et  $\alpha$  sont injectives. Il est donc essentiel de préciser le contexte en parlant d'un produit tensoriel puisque par exemple vous avez vu dans le cours que l'injection  $\iota : \mathbf{Z} \rightarrow \mathbf{Q}$  ne donne pas lieu à une injection  $\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}/n\mathbf{Z}$  dans<sup>38</sup>  $\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/n\mathbf{Z} = \{0\}$  et on aura donc  $1 \otimes_{\mathbf{Z}} 1 \neq 0$  tandis que  $1 \otimes_{\mathbf{Q}} 1 = 0$ . Noter que l'application est ici identiquement nulle et que l'on n'a donc pas que l'image de  $\iota \otimes \text{Id}$  est isomorphe à  $\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/n\mathbf{Z}$ .

35. Obtenu par  $\varphi \mapsto \varphi(1)$ .

36. L'application  $\varphi \mapsto \varphi(1)$  donne un isomorphisme avec  $p\mathbf{Z}/p^2\mathbf{Z}$  et  $\alpha$  est envoyé sur  $p$ .

37. Se rendre compte ici qu'on regarde simplement les morphismes de groupes.

38. Autrement dit, même si  $\mathbf{Z}$  est un sous-module de  $\mathbf{Q}$ , ce n'est pas le cas de  $\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/n\mathbf{Z}$  avec  $\mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{Z}/n\mathbf{Z}$ .

7. Écrivons  $N = \varphi(M) \oplus P$  et considérons  $\pi : N \rightarrow M$  la surjection définie par  $\pi(\varphi(m) + p) = m$ . L'application  $\pi$  est clairement linéaire et vérifie  $\pi \circ \varphi = \text{Id}_M$ . On en déduit des applications linéaires  $\varphi^{\otimes k}$  et  $\pi^{\otimes k}$  telles que (d'après les questions précédentes)

$$\pi^{\otimes k} \circ \varphi^{\otimes k} = (\pi \circ \varphi)^{\otimes k} = \text{Id}_M^{\otimes k} = \text{Id}_{M^{\otimes k}}.$$

On a donc un inverse à gauche et  $\varphi^{\otimes k}$  est surjective.

Un contre-exemple est donné par l'inclusion  $i : I \rightarrow A$  avec  $I = (X, Y)$  et  $A = k[X, Y]$ . On vérifie alors que  $i^{\otimes 2} : I^{\otimes 2} \rightarrow A^{\otimes 2}$  envoie l'élément non nul<sup>39</sup>  $X \otimes Y - Y \otimes X$  de  $I^{\otimes 2}$  sur<sup>40</sup>

$$X \otimes Y - Y \otimes X = XY(1 \otimes 1 - 1 \otimes 1) = 0$$

si bien que  $i^{\otimes 2}$  n'est pas injective. Cela provient du fait que  $I$  n'est pas projectif<sup>41</sup>.

8. En d'autres termes, il s'agit de montrer que

$$\text{Ker}(\varphi \otimes \psi) = (i \otimes \text{Id})(\text{Ker}(\varphi) \otimes_A N) + (\text{Id} \otimes j)(M \otimes_A \text{Ker}(\psi))$$

pour  $i : \text{Ker}(\varphi) \rightarrow M$  et  $j : \text{Ker}(\psi) \rightarrow N$  les inclusions. Il est clair que tout élément de  $U = (i \otimes \text{Id})(\text{Ker}(\varphi) \otimes_A N) + (\text{Id} \otimes j)(M \otimes_A \text{Ker}(\psi))$  est dans le noyau de  $\varphi \otimes \psi$ . On obtient donc un morphisme  $\Phi : (M \otimes_A N)/U \rightarrow M' \otimes_A N'$  dont il s'agit de montrer qu'elle est injective pour conclure. Pour ce faire, construisons un inverse. On a  $\Phi(\overline{m \otimes n}) = \varphi(m) \otimes \psi(n)$ . et par surjectivité de  $\varphi$  et  $\psi$ , tout tenseur pur de  $M' \otimes_A N'$  est de la forme  $\varphi(m) \otimes \psi(n)$  pour un certain  $m \in M$  et un certain  $n \in N$ . Si on choisit deux autres éléments  $m' \in M$  et  $n' \in N$  tels que  $\varphi(m) = \varphi(m')$  et  $\psi(n) = \psi(n')$ , on en déduit que

$$\varphi(m) \otimes \psi(n) = \varphi(m') \otimes \psi(n') + \varphi(m - m') \otimes \psi(n) + \varphi(m) \otimes \psi(n - n') + \varphi(m - m') \otimes \psi(n - n') = \varphi(m') \otimes \psi(n') \pmod{U}$$

car  $m - m'$  est dans le noyau de  $\varphi$  et  $n - n'$  dans celui de  $\psi$ . On a ainsi une application bilinéaire bien définie  $M' \times N' \rightarrow (M \otimes_A N)/U$  définie par  $(m', n') = (\varphi(m), \psi(n)) \mapsto \overline{\varphi(m) \otimes \psi(n)}$  qui donne lieu à une unique application linéaire  $\tilde{\Phi} : M' \otimes_A N' \rightarrow (M \otimes_A N)/U$  dont on vérifie qu'il s'agit de l'inverse de  $\Phi$  ce qui permet de conclure!

**EXERCICE 9.** On considère  $\mathbf{R}$  en tant que  $\mathbf{Z}$ -module.

1. Soit  $y \in \mathbf{R} \setminus \mathbf{Q}$ . Montrer qu'il existe  $\varphi \in \text{Hom}_{\mathbf{Z}}(\mathbf{R}, \mathbf{Q})$  telle que  $\varphi(1) = 0$  et  $\varphi(y) = 1$ .
2. Soient  $x \in \mathbf{R}^\times$  et  $y \in \mathbf{R}$ . Montrer que l'on a

$$x \otimes \bar{y} = 0 \in \mathbf{R} \otimes_{\mathbf{Z}} \mathbf{R}/\mathbf{Z} \iff y \in \mathbf{Q}.$$

3. Soient  $(x_i)_{i \in I}$  une famille  $\mathbf{Q}$ -libre de réels et  $V$  le sous-espace vectoriel de  $\mathbf{R}$  engendré par cette famille. Montrer que si  $1 \notin V$ , alors  $(1 \otimes \bar{x}_i)_{i \in I}$  est une famille  $\mathbf{R}$ -libre de  $\mathbf{R} \otimes_{\mathbf{Z}} \mathbf{R}/\mathbf{Z}$ .

**SOLUTION.**

1. On peut voir  $\mathbf{R}$  comme un  $\mathbf{Q}$ -espace vectoriel. On a alors que la famille  $(1, y)$  est  $\mathbf{Q}$ -libre et on peut<sup>42</sup> la compléter en une  $\mathbf{Q}$ -base  $(1, y, (e_i)_{i \in I})$  de  $\mathbf{R}$ . On considère alors l'application  $\mathbf{Q}$ -linéaire (et donc  $\mathbf{Z}$ -linéaire)  $\varphi : \mathbf{R} \rightarrow \mathbf{Q}$  définie par  $\varphi(1) = \varphi(e_i) = 0$  pour tout  $i \in I$  et  $\varphi(y) = 1$ .
2. Si  $y = \frac{p}{q}$ , on a

$$x \otimes \bar{y} = q \left( \left( \frac{x}{q} \right) \otimes \bar{y} \right) = \left( \frac{x}{q} \right) \otimes (q\bar{y}) = \left( \frac{x}{q} \right) \otimes 0 = 0.$$

Réciproquement, supposons que  $x \otimes \bar{y} = 0$  et supposons que  $y \in \mathbf{R} \setminus \mathbf{Q}$ . On considère alors l'application  $\varphi$  de la question précédente. L'application  $\mathbf{R} \times \mathbf{R}/\mathbf{Z} \rightarrow \mathbf{R}$  définie par  $(x, \bar{y}) \mapsto x\varphi(y)$  est bilinéaire et bien définie car  $\varphi(\mathbf{Z}) = \{0\}$ . Elle induit donc une application linéaire  $f : \mathbf{R} \otimes_{\mathbf{Z}} \mathbf{R}/\mathbf{Z} \rightarrow \mathbf{R}$  telle que  $f(x \otimes \bar{y}) = x\varphi(y)$ . Mais, si  $y \notin \mathbf{Q}$  et  $x \neq 0$ , il vient que  $f(x \otimes \bar{y}) = x\varphi(y) = x = 0$  ce qui est absurde. Ainsi  $y \in \mathbf{Q}$  et on a l'équivalence.

39. Voir l'exercice 3.

40. Bien voir ici que la subtilité provient du fait que  $1 \in A$  mais que  $1 \notin I$ .

41. Par exemple car  $0 \rightarrow k[X, Y] \xrightarrow{f} k[X, Y] \oplus k[X, Y] \xrightarrow{g} I \rightarrow 0$  avec  $f(P) = (YP, -XP)$  et  $g(P, Q) = PX + QY$  n'est pas scindée.

42. Modulo l'axiome du choix!

3. Soit  $(\lambda_i)_{i \in I} \in \mathbf{R}^{(I)}$  tels que

$$\sum_{i \in I} \lambda_i (1 \otimes \bar{x}_i) = 0.$$

On a alors par hypothèse ( $1 \notin V$ ) que chaque  $x_i$  est irrationnel et par la question 1. il existe pour tout  $i \in I$  une application  $\mathbf{Z}$ -linéaire  $\varphi_i : \mathbf{R} \rightarrow \mathbf{Q}$  telle que  $\varphi_i(1) = 0$  et  $\varphi_i(x_i) = 1$  tandis que  $\varphi_i(x_j) = 0$  pour  $j \neq i$ . On a alors comme en 2., une application linéaire  $f_i : \mathbf{R} \otimes_{\mathbf{Z}} \mathbf{R}/\mathbf{Z} \rightarrow \mathbf{R}$  telle que  $f_i(x \otimes \bar{y}) = x\varphi_i(y)$ . On a donc

$$0 = f_i \left( \sum_{i \in I} \lambda_i (1 \otimes \bar{x}_i) \right).$$

Mais la structure de  $\mathbf{R}$ -espace vectoriel sur  $\mathbf{R} \otimes_{\mathbf{Z}} \mathbf{R}/\mathbf{Z}$  est donnée par

$$t \cdot (x \otimes \bar{y}) = (tx) \otimes \bar{y}$$

si bien que

$$0 = f_i \left( \sum_{i \in I} (\lambda_i \otimes \bar{x}_i) \right) = \sum_{i \in I} f_i(\lambda_i \otimes \bar{x}_i) = \lambda_i$$

de sorte qu'on a la résultat.