Examen 2021/2022 (I) - Correction
4M003 - Algèbre commutative
Anna Cadoret

Exercice 1. Soit k un corps de caractéristique 0 et V un k-espace vectoriel de dimension finie $d \geq 2$ sur k. On note $T^0(V) := k$, $T^1(V) := V$ et $T^{n+1}(V) := V \otimes_k T^n(V)$, $n \geq 1$.

(1) Pour $\sigma \in \mathcal{S}_n$ l'application $V^n \to T^n(V)$, $(v_1, \cdots, v_n) \mapsto v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(n)})$ est n-k-linéaire donc, par prop. univ. du produit tensoriel se factorise en un morphisme de k-modules $T^n(\sigma) : T^n(V) \to T^n(V)$. On vérifie immédiatement sur les générateurs de la forme $v_1 \otimes \cdots \otimes v_n$ du k-ev $T^n(V)$ les relations ($T^n(Id) = Id$ et) $T^n(\sigma)T^n(\tau) = T^n(\sigma\tau)$.

(2) On note $R^n(V) \subset T^n(V)$ le sous-k-espace vectoriel engendré par les éléments de la forme $t - \sigma \cdot t$, $t \in T^n(V)$, $S^n(V) := T^n(V)/R^n(V)$ et $\pi_n : T^n(V) \twoheadrightarrow S^n(V)$ la projection canonique. Soit W un k-espace vectoriel et $f : V^n \to W$ une application n-k-multilinéaire symmétrique. S'il existe un morphisme de k-ev $S^n(f) : S^n(V) \to W$ tel que $S^n(f) \circ p_n = f$, on a nécessairement $S^n(f)(v_1 \cdot \cdots \cdot v_n) = f(v_1, \ldots, v_n)$ or, comme les éléments de la forme $v_1 \cdot \cdots \cdot v_n$ engendre $S^n(V)$ comme k-ev, cela montre que, s'il existe, $S^n(f) : S^n(V) \to W$ est unique. Pour l'existence, par prop. univ. du produit tensoriel l'application k-n-linéaire $f : V^n \to W$ se factorise en un morphisme de k-ev $T^n(f) : T^n(V) \to W$. Par symmétrie, $R^n(V) \subset \ker(T^n(f))$ donc, par prop. univ. du quotient, le morphisme de k-ev $T^n(f) : T^n(V) \to W$ se factorise en un morphisme de k-ev $S^n(f) : S^n(V) = T^n(V)/R^n(V) \to W$.

(3) On vérifie immédiatement que $R^m(V) \times R^n(V) \subset \ker(T^m(V) \times T^n(V) \to T^{m+n}(V) \twoheadrightarrow S^{m+n}(V))$ et on applique la prop. univ. du quotient pour obtenir la factorisation

$$\begin{tikzcd}
T^m(V) \times T^n(V) \arrow[r] \arrow[d, two heads] & T^{m+n}(V) \arrow[d, two heads] \\
S^m(V) \times S^n(V) \arrow[r] & S^{m+n}(V)
\end{tikzcd}$$

Cela munit $S^*(V)$ d'une structure de k-algèbre commutative de zéro celui du k-module $S^*(V)$ et d'unité $1 \in k = S^0(V) \subset S^*(V)$.

(4) Soit A une k-algèbre commutative et $f : V \to A$ un morphisme de k-modules. S'il existe un morphisme de k-algèbres $S^*(f) : S^*(V) \to A$ tel que $S^*(f) \circ \iota_V = f$, on a nécessairement $S^*(f)(v_1 \cdot \cdots \cdot v_n) = S^*(f)(\iota_V(v_1) \cdots \iota_V(v_n)) = S^*(f)(\iota_V(v_1)) \cdots S^*(f)(\iota_V(v_n)) = f(v_1) \cdots f(v_n)$ or, comme les éléments de la forme $v_1 \cdot \cdots \cdot v_n$ engendre $S^*(V)$ comme k-ev, cela montre que, s'il existe, $S^*(f) : S^n(V) \to A$ est unique. Pour l'existence, pour chaque $n \geq 1$, par prop. univ. de $p_n : V^n \to S^n(V)$, l'application n-k-linéaire symmétrique $V^n \to A$, $(v_1, \ldots, v_n) \mapsto f(v_1) \cdots f(v_n)$ se factorise en un morphisme de k-ev $S^n(f) : S^n(V) \to A$, $v_1 \cdot \cdots \cdot v_n \mapsto f(v_1) \cdots f(v_n)$ et on vérifie immédiatement sur les générateurs de la forme $v_1 \cdot \cdots \cdot v_n$ que $S^*(f) := \oplus_{n \geq 0} S^n(f) : S^*(V) \to A$ est un morphisme de k-algèbres tq $S^*(f) \circ \iota_V = f$.

(5) Notons $f : V \hookrightarrow k[X_1, \ldots, X_d]$ le morphisme de k-modules défini par $f(v_i) = X_i$. D'après (5), il existe un unique morphisme de k-algèbres $\Phi := S^*(f) : S^*(V) \to k[X_1, \ldots, X_d]$ tq $S^*(f)(v_i) = X_i$, $i = 1, \ldots, d$. Inversement, par prop. univ de $\iota_k : k \hookrightarrow k[X_1, \ldots, X_d]$, il existe un unique morphisme de k-algèbres $\Psi : k[X_1, \ldots, X_d] \to S^*(V)$ tq $\Psi(X_i) = v_i$, $i = 1, \ldots, d$. Par construction $\Psi \circ \Phi(v_i) = v_i$, $i = 1, \ldots, d$ donc $\Psi \circ \Phi = Id$ puisque $v_1, \ldots, v_d$ engendrent $S^*(V)$ comme k-algèbre et $\Phi \circ \Psi(X_i) = X_i$, $i = 1, \ldots, d$ donc $\Phi \circ \Psi = Id$ puisque $X_1, \ldots, X_d$ engendrent $k[X_1, \ldots, X_d]$ comme k-algèbre.

Exercice 2. Soit $n, r \geq 1$ des entiers. On note $S(n, r)$ le nombre de sous-$\mathbb{Z}$-modules $M \subset (\mathbb{Z}/n)^{\oplus r}$ de cardinal $\leq n$. L'objectif de cet exercice est de montrer qu'il existe une constante $\alpha(r) > 0$ telle que $S(n, r) \leq n^{\alpha(r)}$.

(1) Par th. de structure des modules de type fini sur les anneaux principaux (ici, $\mathbb{Z}$) il existe une unique suite d'entiers positifs $d_1|d_2|\cdots|d_s$ telle que $M \simeq \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_s$. En outre, comme M est un sous $\mathbb{Z}$-module de $(\mathbb{Z}/n)^{\oplus r}$, chaque élément de M est d'ordre divisant n (plus précisément, si on écrit $\underline{a} = (a_1, \dots, a_r) \in (\mathbb{Z}/n)^{\oplus r}$ avec $a_i \in \mathbb{Z}/n$, $i = 1, \dots, r$, l'ordre de $\underline{a}$ est le ppcm des ordres des a_i, $i = 1, \dots, r$); en particulier $d_s|n$. Enfin, fIxons un premier $p|d_s$ et notons $\mu_1 \leq \cdots \leq \mu_s$ la multiplicité de p dans $d_1, \dots, d_s$ respectivement et $\mu \geq \mu_s$ la multiplicité de p dans n. Par le lemme Chinois, $M \simeq M' \times (\mathbb{Z}/p^{\mu_1} \times \cdots \mathbb{Z}/p^{\mu_s})$ et $(\mathbb{Z}/n)^{\oplus r} \simeq N' \times (\mathbb{Z}/p^{\mu})^{\oplus r}$ avec M', N' tous deux d'ordre premier à p. Puisqu'il n'y a pas de morphisme de $\mathbb{Z}$-modules non trivial entre deux $\mathbb{Z}$-modules finis d'ordre premier entre eux, l'inclusion canonique $M \hookrightarrow (\mathbb{Z}/n)^{\oplus r}$ se restreint en un morphisme injectif de $\mathbb{Z}$-modules $\mathbb{Z}/p^{\mu_1} \times \cdots \mathbb{Z}/p^{\mu_s} \hookrightarrow (\mathbb{Z}/p^{\mu})^{\oplus r}$. La multiplication par p induit le diagramme canonique exact de morphismes de $\mathbb{Z}$-modules

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & (\mathbb{Z}/p)^{\oplus s} \arrow[r] \arrow[d] & (\mathbb{Z}/p)^{\oplus r} \arrow[r] \arrow[d] & C[p] \arrow[d] & \\
0 \arrow[r] & \mathbb{Z}/p^{\mu_1} \times \cdots \mathbb{Z}/p^{\mu_s} \arrow[r] \arrow[d, "p"] & (\mathbb{Z}/p^{\mu})^{\oplus r} \arrow[r] \arrow[d, "p"] & C \arrow[r] \arrow[d, "p"] & 0 \\
0 \arrow[r] & \mathbb{Z}/p^{\mu_1} \times \cdots \mathbb{Z}/p^{\mu_s} \arrow[r] & (\mathbb{Z}/p^{\mu})^{\oplus r} \arrow[r] & C \arrow[r] & 0
\end{tikzcd}$$

En particulier, on a un morphisme injectif de $\mathbb{F}_p$-ev $(\mathbb{Z}/p)^{\oplus s} \hookrightarrow (\mathbb{Z}/p)^{\oplus r}$, ce qui force $s \leq r$.

(2) L'isomorphisme $\mathrm{Hom}_{\mathbb{Z}}(M, (\mathbb{Z}/n)^{\oplus r}) \tilde{\to} \prod_{1 \leq i \leq s} \mathrm{Hom}(\mathbb{Z}/d_i, (\mathbb{Z}/n)^{\oplus r})$ est la prop. univ. de la somme directe appliquée à $\oplus_{1 \leq i \leq s} \mathbb{Z}/d_i$ et l'isomorphisme $\mathrm{Hom}(\mathbb{Z}/d_i, (\mathbb{Z}/n)^{\oplus r}) \tilde{\to} \mathrm{Hom}(\mathbb{Z}/d_i, (\mathbb{Z}/n))^r$ est la prop. univ. du produit appliquée à $(\mathbb{Z}/n)^{\oplus r} = (\mathbb{Z}/n)^r$.

(3) Comme $\mathbb{Z}/d_i$ est engendré comme $\mathbb{Z}$-module par $\overline{1}$, l'évaluation en $\overline{1}$ induit un morphisme injectif de $\mathbb{Z}$-modules $\mathrm{Hom}(\mathbb{Z}/d_i, \mathbb{Z}/n) \hookrightarrow \mathbb{Z}/n$. De plus, pour tout $\phi \in \mathrm{Hom}(\mathbb{Z}/d_i, \mathbb{Z}/n)$, $\phi(\overline{1})$ est d'ordre divisant d_i donc l'image de $\mathrm{Hom}(\mathbb{Z}/d_i, \mathbb{Z}/n) \hookrightarrow \mathbb{Z}/n$ est contenue dans

$$\ker(d_i \cdot : \mathbb{Z}/n \to \mathbb{Z}/n) = q_i\mathbb{Z}/n \simeq \mathbb{Z}/d_i.$$

(où on a noté $q_i := n/d_i$). Inversement, tout élément $a \in q_i\mathbb{Z}/n \simeq \mathbb{Z}/d_i$ définit un unique morphisme de $\mathbb{Z}$-module $\phi_a\, \mathbb{Z}/d_i \to \mathbb{Z}/n$, $\overline{1} \mapsto a$. On en déduit que $\mathrm{Hom}(\mathbb{Z}/d_i, \mathbb{Z}/n) \tilde{\to} \mathbb{Z}/d_i$. En particulier $|\mathrm{Hom}(\mathbb{Z}/d_i, \mathbb{Z}/n)| = d_i$.

(4) Par (1), le nombre de sous-$\mathbb{Z}$-modules de $(\mathbb{Z}/n)^{\oplus r}$ d'ordre divisant n est majoré par le nombre de morphismes injectifs de $\mathbb{Z}$-modules $\mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_s \hookrightarrow (\mathbb{Z}/n)^{\oplus r}$, avec $d_1|d_2|\cdots|d_s$ tels que $d_s|n$ et $s \leq r$. Le nombre de morphismes injectifs est lui-même majoré par le nombre total de morphismes de $\mathbb{Z}$-modules $\mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_s \to (\mathbb{Z}/n)^{\oplus r}$. Par (2) et (3), à $d_1|d_2|\cdots|d_s$ tels que $d_s|n$ et $s \leq r$ fixés on a $\prod_{1 \leq i \leq s} d_i^r = (d_1 \cdots d_s)^r \leq n^r$ morphismes de $\mathbb{Z}$-modules $\mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_s \to (\mathbb{Z}/n)^{\oplus r}$. Enfin, le nombre de suites d'entiers positifs $d_1|d_2|\cdots|d_s$ tels que $d_s|n$ et $s \leq r$ est majoré par $d(n)^r$. On en déduit $S(n, r) \leq d(n)^r n^r$.

(5) Il suffit d'observer que $d(n) \leq n$ et dc prendre $\alpha(r) = 2$.

Exercice 3.

(1) Cela résulte du fait (vu en cours) que les applications $\mathfrak{q} \mapsto c_{\mathfrak{p}}^{-1}\mathfrak{q}$ et $\mathfrak{q} \mapsto c_{\mathfrak{p}}(\mathfrak{q})A_{\mathfrak{p}}$ induisent des bijections inverses l'une de l'autre et préservant l'inclusion entre *spec*$(A_{\mathfrak{p}})$ et les idéaux premiers de A contenu dans $\mathfrak{p}$.

(2) On note $p : A \twoheadrightarrow A/Aa$ le morphisme quotient. Les applications $\mathfrak{q} \mapsto p^{-1}(\mathfrak{q})$ et $\mathfrak{q} \mapsto p(\mathfrak{q})$ induisent des bijections inverses l'une de l'autre et préservant l'inclusion entre *spec*(A/Aa) et les idéaux premiers de A contenant Aa. *Via* cet bijection, les éléments minimaux de $\mathcal{P}_a$ correspondent donc aux idéaux premiers minimaux de A/Aa. Or comme tout quotient d'un anneau noetherien est noetherien, A/Aa est

noetherien dc d'après le rappel de l'énoncé, ne contient qu'un nbr fin d'idéaux premiers minimaux.

(3) C'est l'argument du lemme de Nakayama. On renvoie aux TDs.

(4) On suppose ici A local d'unique idéal maximal $\mathfrak{m}$ et $\mathfrak{m}$ nilpotent. Disons $\mathfrak{m}^N = 0$. On a donc une suite de sec de A-modules:

$$0 \to \mathfrak{m} \to A \to A/\mathfrak{m} \to 0$$
$$0 \to \mathfrak{m}^2 \to \mathfrak{m} \to \mathfrak{m}/\mathfrak{m}^2 \to 0$$
$$\cdots$$
$$0 \to \mathfrak{m}^{N-1} \to \mathfrak{m}^{N-2} \to \mathfrak{m}^{N-2}/\mathfrak{m}^{N-1} \to 0$$

Les termes de droite sont des $A/\mathfrak{m}$-modules noetheriens donc de $A/\mathfrak{m}$-dim finie donc artiniens. Comme $\mathfrak{m}^N = 0$, $\mathfrak{m}^{N-1}$ est aussi un $A/\mathfrak{m}$-module noetherien donc de $A/\mathfrak{m}$-dim finie donc artinien. En utilisant que dans une sec

$$0 \to M' \to M \to M'' \to 0$$

M est artinien si (et seulement si) M' et M'' le sont, on conclut par récurrence (en partant de la dernière sec ci-dessus).

(5) D'après (1) $ht(A_\mathfrak{p}) = ht(A)$ dc quitte à remplacer A par $A_\mathfrak{p}$, opsq A est local d'unique idéal maximal $\mathfrak{p}$.

(6) Supposons que pour tout idéal premier $\mathfrak{q} \in spec(A)$, $\mathfrak{q} \subsetneq \mathfrak{p}$, $\mathfrak{q}A_\mathfrak{q}$ est nilpotent. Comme $A_\mathfrak{q}$ est encore noetherien, par (4), on a $A_\mathfrak{q}$ artinien dc, par le rappel de l'énoncé, $ht(\mathfrak{q}A_\mathfrak{q}) = 0$ et, en invoquant à nouveau (1), $ht(\mathfrak{q}) = ht(\mathfrak{q}A_\mathfrak{q}) = 0$. Cela montre bien que $ht(\mathfrak{p}) = 1$.

(7) On a

$$\sqrt{Aa} = \bigcap_{\mathfrak{q} \in spec(A) \mid a \in \mathfrak{q}} \mathfrak{q} = \bigcap_{\mathfrak{q} \in \mathcal{P}_a} \mathfrak{q}.$$

Mais on s'est ramené au cas où A est local d'unique idéal maximal $\mathfrak{p}$ *avec* $\mathfrak{p} \in \mathcal{P}_a$. Dc $\mathcal{P}_a = \{\mathfrak{p}\}$!

(8) Comme A est noetherien, $\sqrt{Aa}$ est de type fini. Soit $x_1, \ldots, x_r$ un système de générateurs de $\sqrt{Aa}$ comme idéal. On peut toujours trouver $N \gg 0$ tq $x_i^N \in Aa$, $i = 1, \ldots, r$. Mais alors, pour $x = \sum_{1 \leq i \leq r} a_i x_i \in \sqrt{Aa}$ arbitraire, x^{Nr} est combinaison A-linéaire d'éléments de la forme $x_1^{k_1} \cdots x_r^{k_r}$ avec $k_1 + \cdots + k_r = Nr$ donc, nécessairement, au moins l'un des k_i est $> N$.

(9) L'anneau A/Aa est noetherien, local d'unique idéal maximal $\mathfrak{p}/Aa$. D'après (7) $\mathfrak{p}/Aa = \sqrt{0}$ et d'après (8), $\sqrt{0}$ est nilpotent. On conclut par (4).

(10) On note $\mathfrak{q}^{(n)} := c_\mathfrak{q}^{-1}(\mathfrak{q}^n A_\mathfrak{q}) \subset A$. Par construction $\mathfrak{q}^{(n)} \supset \mathfrak{q}^{(n+1)} \supset \cdots$ donc, comme A/a est artinien par (9), il existe un entier $n \geq 1$ tel que $p(\mathfrak{q}^{(n)}) = p(\mathfrak{q}^{(n+1)})$ *i.e.* $\mathfrak{q}^{(n)} + Aa = \mathfrak{q}^{(n+1)} + Aa$. Comme $\mathfrak{q}^{(n+1)} + a\mathfrak{q}^{(n)} \subset \mathfrak{q}^{(n)}$, il suffit de mq $\mathfrak{q}^{(n)} \subset \mathfrak{q}^{(n+1)} + a\mathfrak{q}^{(n)}$. On utilise que comme $\mathfrak{q} \subsetneq \mathfrak{p}$ et $\mathfrak{p} \in \mathcal{P}_a$, $a \notin \mathfrak{q}$. En effet, pour tout $x_n \in \mathfrak{q}^{(n)}$, écrivons $x_n = x_{n+1} + \alpha a$ avec $x_{n+1} \in \mathfrak{q}^{(n+1)}$ et $\alpha \in A$. On a dc $c_\mathfrak{q}(\alpha)c_\mathfrak{q}(a) = c_\mathfrak{q}(x_n - x_{n+1}) \in \mathfrak{q}^n A_\mathfrak{q}$ or comme $c_\mathfrak{q}(a) \in A_\mathfrak{q}^\times$, $c_\mathfrak{q}(\alpha) = c_\mathfrak{q}(a)^{-1} c_\mathfrak{q}(x_n - x_{n+1}) \in \mathfrak{q}^n A_\mathfrak{q}$. Autrement dit, $\alpha \in c_\mathfrak{q}^{-1}(\mathfrak{q}^n A_\mathfrak{q}) = \mathfrak{q}^{(n)}$.

(11) Comme $\mathfrak{q}^{(n)}$, $\mathfrak{q}^{(n+1)}$ sont des idéaux, il résulte de (10) que $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$ dc, comme $\mathfrak{q}^n A_\mathfrak{q}$ est engendré comme idéal de $A_\mathfrak{q}$ par $c_\mathfrak{q}(\mathfrak{q}^{(n)})$, que $\mathfrak{q}^n A_\mathfrak{q} = \mathfrak{q}^{n+1} A_\mathfrak{q}$. Mais cette dernière égalité se réécrit aussi $\mathfrak{q}^n A_\mathfrak{q} = \mathfrak{q}\mathfrak{q}^n A_\mathfrak{q}$. Comme $M = \mathfrak{q}^n A_\mathfrak{q} \subset A_\mathfrak{q}$ est un idéal de l'anneau noetherien $A_\mathfrak{q}$, il est de type fini comme $A_\mathfrak{q}$-module. Comme $\mathfrak{q}$ est l'unique idéal maximal de $A_\mathfrak{q}$, il coincide avec le radical de Jacobson de $A_\mathfrak{q}$. Donc, par (3), $\mathfrak{q}^n A_\mathfrak{q} = 0$, qui est bien ce que l'on voulait montrer (*cf.* (6)).