Compléments sur les anneaux

Travaux dirigés du 9 et du 12 décembre 2025

Exercice 1. Un contre-exemple

Soient V le k-espace vectoriel $k^{(\mathbb{N})}$ et $A = \mathrm{End}_k(V)$. Montrer que les A-modules A et A^2 sont isomorphes.

Si V est un k-espace vectoriel quelconque qui s'écrit comme une somme directe de sous-espaces vectoriels $V = V_1 \oplus V_2$, on a une bijection $\Phi : A = \mathrm{End}_k(V) \xrightarrow{\sim} \mathrm{Hom}_k(V_1, V) \times \mathrm{Hom}_k(V_2, V)$ qui correspond aux restrictions à V_1 et V_2. On peut munir les $\mathrm{Hom}_k(V_i, V)$ de structures de A-modules par composition à gauche et ces structures font de Φ un isomorphisme de A-modules.

Dans le cas qui nous intéresse, en notant $(e_n)_{n\in\mathbb{N}}$ la base canonique de $V = k^{(\mathbb{N})}$, on dispose d'une décomposition $V = V_1 \oplus V_2$ avec $V_1 = \mathrm{vect}(e_{2n})_{n\in\mathbb{N}}$ et $V_2 = \mathrm{vect}(e_{2n+1})_{n\in\mathbb{N}}$. L'intérêt de cette décomposition est que l'on a a des isomorphismes $\alpha_1 : V \xrightarrow{\sim} V_1$, $e_n \mapsto e_{2n}$ et $\alpha_2 : V \xrightarrow{\sim} V_2$, $e_n \mapsto e_{2n+1}$, dont on déduit des bijections $\mathrm{Hom}_k(V_i, V) \to \mathrm{End}_k(V)$ en précomposant par les α_i. Ces bijections étant A-linéaires, on en déduit un isomorphisme de A-modules $A \simeq A^2$.

Exercice 2. Anneau opposé

Si $(A, +, \cdot)$ est un anneau, on peut regarder la loi de composition inversée $x \star y = y \cdot x$ sur A et définir l'*anneau opposé* $A^{\mathrm{opp}} := (A, +, \star)$. Si l'anneau A est commutatif, on a bien sûr $A = A^{\mathrm{opp}}$. Si M est un A-module, on notera $\mathrm{End}_A(M)$ l'anneau des endomorphismes A-linéaires de M. Soit $n \geq 1$ un entier.

1. Montrer que l'on a un isomorphisme d'anneaux $\mathrm{M}_n(A)^{\mathrm{opp}} \simeq \mathrm{M}_n\left(A^{\mathrm{opp}}\right)$. Qu'en déduire si A est commutatif ?

   On note $\star$ la multiplication dans $\mathrm{M}_n(A)^{\mathrm{opp}}$ et $\circ$ celle dans $\mathrm{M}_n\left(A^{\mathrm{opp}}\right)$. Pour qu'une bijection $f : \mathrm{M}_n\left(A^{\mathrm{opp}}\right) \xrightarrow{\sim} \mathrm{M}_n(A)^{\mathrm{opp}}$ soit un isomorphisme d'anneaux, il suffit qu'elle vérifie $f(M) \star f(M') = f(M \circ M')$ pour tous M, M'. Or on calcule

   $$\left(f(M) \star f(M')\right)_{i,k} = \left(f(M')f(M)\right)_{i,k} = \sum_j \left(f(M')\right)_{i,j} \left(f(M)\right)_{j,k} = \sum_j \left(f(M)\right)_{j,k} \star \left(f(M')\right)_{i,j}.$$

   En prenant $f(M) = {}^tM$, on obtient

   $$\left(f(M) \star f(M')\right)_{i,k} = \sum_j M_{k,j} \star M'_{j,i} = (M \bullet M')_{k,i} = \left(f(M \bullet M')\right)_{i,k},$$

   ce qui conclut la première partie de la question. Si A est commutatif, on a donc $\mathrm{M}_n(A)^{\mathrm{opp}} \simeq \mathrm{M}_n(A)$.

2. Montrer que $u \mapsto u(1)$ induit un isomorphisme d'anneaux $\mathrm{End}_A(A) \xrightarrow{\sim} A^{\mathrm{opp}}$.

   Si $u \in \mathrm{End}_A(A)$, pour tout $a \in A$ on a $u(a) = u(a \cdot 1) = a \cdot u(1)$ donc l'application est bijective. De plus, on déduit du calcul que $u \circ v(1) = u(v(1) \cdot 1) = v(1) \cdot u(1)$. Comme on a aussi $\mathrm{id}(1) = 1$ et $(u + v)(1) = u(1) + v(1)$, l'application est un isomorphisme d'anneaux.

3. Plus généralement, soient M un A-module libre de rang n et $e_1, \ldots, e_n$ une base de M. Pour $u \in \mathrm{End}_A(M)$ on note $\mathrm{Mat}_e\, u = \left(u_{i,j}\right) \in \mathrm{M}_n(A)$ l'élément déterminé par les relations $u\left(e_j\right) = \sum_{i=1}^n u_{i,j} e_i$, pour $1 \leqslant j \leqslant n$. Montrer que

   $$\mathrm{End}_A(M) \to \mathrm{M}_n\left(A^{\mathrm{opp}}\right),\ u \mapsto \mathrm{Mat}_e\, u$$

   est un isomorphisme d'anneaux.

   L'application est bijective, additive, et envoie 1 sur 1. De plus, on calcule

   $$u \circ v(e_k) = u\left(\sum_j v_{j,k} e_j\right) = \sum_j v_{j,k} u(e_j) = \sum_j v_{j,k} \sum_i u_{i,j} e_i = \sum_i \sum_j v_{j,k} u_{i,j} e_i = \sum_i \sum_j u_{i,j} \star v_{j,k} e_i,$$

   d'où $(\mathrm{Mat}_e(u \circ v))_{i,k} = \sum_j (\mathrm{Mat}_e\, u)_{i,j} \star (\mathrm{Mat}_e\, v)_{j,k} = (\mathrm{Mat}_e\, u \bullet \mathrm{Mat}_e\, v)_{i,k}$, ce qui conclut.

Exercice 3. Théorème de la base de Hilbert

On se propose de montrer que si A est un anneau (commutatif) noethérien, alors $A[X]$ aussi. Procédons par contraposée en se donnant un anneau commutatif A tel que $A[X]$ n'est pas noethérien. Soit I un idéal de $A[X]$ qui n'est pas finiment engendré. On construit par récurrence une suite $(P_n)_{n\in\mathbb{N}}$ d'éléments de $A[X]$ en prenant P_0 de degré minimal dans I et pour $n \geq 1$, P_n de degré minimal dans $I - (P_0, \ldots, P_{n-1})$. On obtient une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A en prenant a_n le coefficient dominant de P_n pour tout $n \geq 0$.

1. Montrer que la suite croissante $(J_n)_{n\in\mathbb{N}}$ d'idéaux de A, définie par $J_n = (a_0,\dots,a_n)$ pour $n \geq 0$, n'est pas stationnaire.
   On note $d_n = \deg P_n$ pour $n \in \mathbb{N}$, la suite $(d_n)_{n\in\mathbb{N}}$ est croissante par définition des P_n. Supposons la suite $(J_n)_{n\in\mathbb{N}}$ stationnaire, il existe donc $n \in \mathbb{N}$ tel que $a_{n+1} \in (a_0,\dots,a_n)$. On peut donc trouver $\lambda_1,\dots,\lambda_n \in A$ tels que $a_{n+1} = \sum_{i=0}^n \lambda_i a_i$. Alors le polynôme $Q := P_{n+1} - \sum_{i=0}^n \lambda_i X^{d_{n+1}-d_i} P_i \in I$ est de degré strictement inférieur à celui de P_{n+1}, donc est dans $(P_0,\dots,P_n)$. Mais alors, $P_{n+1} = Q + \sum_{i=0}^n \lambda_i X^{d_{n+1}-d_i} P_i \in (P_0,\dots,P_n)$; absurde !
2. En déduire que A n'est pas noethérien.
   On utilise la caractérisation des anneaux noethériens avec les suites croissantes d'idéaux.
3. En déduire que si A est un anneau noethérien, alors $A[X_1,\dots,X_d]$ est noethérien pour tout $d \geq 1$.
   Comme $A[X_1,\dots,X_{d+1}] = A[X_1,\dots,X_d][X_{d+1}]$, on conclut par récurrence sur d.

Exercice 4. Anneaux intégralement clos

Soit A un anneau intègre de corps de fractions K. On note $\widetilde{A}$ l'ensemble des éléments $x \in K$ tels qu'il existe $P \in A[X]$ unitaire avec $P(x) = 0$. On a toujours $A \subseteq \widetilde{A}$. On dit que A est *intégralement clos* si on a $A = \widetilde{A}$.

1. Montrer qu'un anneau factoriel est intégralement clos.
   Soit $x \in \widetilde{A}$, il existe $P = X^n + \lambda_{n-1}X^{n-1} + \cdots + \lambda_0$ qui annule x. On peut écrire $x = \frac{a}{b}$ avec $a \in A$, $b \in A - \{0\}$. On obtient $\left(\frac{a}{b}\right)^n + \lambda_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + \lambda_0 = 0$ et donc $a^n = -\lambda_{n-1}a^{n-1}b - \cdots - \lambda_0 b^n$ et $b \mid a^n$, mais par factorialité de A on peut supposer a et b premiers entre eux. Dans ce cas, on obtient $b \mid a$ d'où $x \in A$, ce qui conclut.

Soit k un corps.

2. Soit A le sous-anneau de $k[X]$ formé des P vérifiant $P(0) = P(1)$. Montrer que A n'est pas intégralement clos.
   On remarque que $X(X-1) \in A$, et donc $X(X-1)k[X] \subseteq A \subseteq k[X]$ puis $\operatorname{Frac} k[X] = \operatorname{Frac} A$ donc il s'agit de trouver un élément de $k(X) - A$ qui annule un polynôme unitaire à coefficients dans A. On remarque que $X \in k(X) - A$ annule $Y(Y-1) - X(X-1) \in A[Y]$, ce qui conclut.
3. Soit A le sous-anneau de $k[X]$ formé des P vérifiant $P'(0) = 0$. Montrer que A n'est pas intégralement clos.
   Le raisonnement est analogue à celui de la question précédente : on remarque que $X^2 \in A$, et donc $\operatorname{Frac} k[X] = \operatorname{Frac} A$ et il s'agit de trouver un élément de $k(X) - A$ qui annule un polynôme unitaire à coefficients dans A ; on remarque que $X \in k(X) - A$ annule $Y^2 - X^2 \in A[Y]$, ce qui conclut.

Exercice 5. Caractérisation de Motzkin-Samuel des anneaux euclidiens

Soit A un anneau commutatif. On définit par récurrence une suite de sous-ensembles $\{\mathrm{E}_n(A)\}_{n\geqslant 0}$ de A en posant $\mathrm{E}_0(A) = \varnothing$, $\mathrm{E}'_n(A) = \mathrm{E}_n(A) \cup \{0\}$ et

$$\mathrm{E}_{n+1}(A) = \left\{a \in A \mid aA + \mathrm{E}'_n(A) = A\right\}$$

On pose aussi $\mathrm{Eucl}(A) = \bigcup_{n\geqslant 0} \mathrm{E}_n(A)$, et pour $a \in \mathrm{Eucl}(A)$ on note $v(a)$ le plus petit entier $n \geqslant 0$ vérifiant $a \in \mathrm{E}_{n+1}(A)$.

1. Déterminer $\mathrm{E}_n(\mathbb{Z})$ pour tout entier $n \geqslant 1$, ainsi que v.
   On constate que l'on a $\mathrm{E}_n(\mathbb{Z}) = \left\{k \in \mathbb{Z} \,|\, 0 < |k| < 2^n\right\}$. En effet, c'est clair pour $n = 0$. De plus, pour $m \in \mathbb{Z}$ on constate que $\mathbb{Z}/m\mathbb{Z}$ est recouvert par les classes des entiers $\pm k$ avec $|k| < 2^n$ si et seulement si on a $0 < |m| < 2^{n+1}$, et on conclut par récurrence. Enfin, pour $m \in \mathbb{Z}$ non nul on a montré que $v(m)$ est le plus petit entier n tel que $|m| < 2^{n+1}$. Autrement dit, $v(m)$ vaut le nombre de chiffres de m dans son écriture en base 2, moins 1 .
2. Pour k un corps, déterminer $\mathrm{E}_n(k[X])$ pour tout entier $n \geqslant 1$, ainsi que v.
   Par division euclidienne, on constate par récurrence sur $n > 0$ que $\mathrm{E}_n(k[X])$ est l'ensemble des polynômes non nuls et de degré $\leqslant n$ dans $k[X]$. On a donc $v = \deg$.
3. Montrer $\mathrm{E}_1(A) = A^\times$ et que $\{\mathrm{E}_n(A)\}_{n\geqslant 0}$ est croissante pour l'inclusion.
   On a $x \in \mathrm{E}_1(A) \iff Ax = A \iff x \sim 1 \iff x \in A^\times$. On a clairement $\mathrm{E}_0(A) \subseteq \mathrm{E}_1(A)$ et $\mathrm{E}_1(A) = A^\times \subseteq \mathrm{E}_2(A)$. Mais pour $X, Y \subseteq A$ avec $X \subseteq Y$, et $a \in A$, alors $aA + X = A$ implique $aA + Y = A$. On en déduit $\mathrm{E}_n(A) \subseteq \mathrm{E}_{n+1}(A)$ pour tout $n \geqslant 0$ par récurrence sur n.
4. On suppose A euclidien pour le stathme φ. Montrer $v \leqslant \varphi$ et $A = \mathrm{Eucl}(A) \cup \{0\}$.
   Soit $a \in A$ non nul avec $\varphi(a) \leqslant n$. Il suffit de montrer que l'on a $v(a) \leqslant n$, i.e. $a \in \mathrm{E}_{n+1}(A)$. On procède par récurrence sur $n \geqslant 0$. Supposons $n = 0$. Par euclidianité et $\varphi(a) = 0$, on a $1 = aq + r$ avec $r = 0$, donc $a \in A^\times = \mathrm{E}_1(A)$ par la question précédente. Pour n général, on constate par euclidianité que A/aA est recouvert par les classes de 0 et des $b \in A$ non nuls avec $\varphi(b) < \varphi(a) \leqslant n$. Par récurrence, un tel b est dans $\mathrm{E}_n(A)$, ce qui montre bien que a est dans $\mathrm{E}_{n+1}(A)$.

5. Réciproquement, montrer que si on a $A = \mathrm{Eucl}(A) \cup \{0\}$ alors A est euclidien pour le stathme v.

   Supposons enfin $A = \mathrm{Eucl}(A) \cup \{0\}$, de sorte que v est bien définie sur $A - \{0\}$. Soient $a, b \in A$ avec $b \neq 0$. Posons $n = v(b)$. On a $b \in \mathrm{E}_{n+1}(A)$ donc la classe de a dans A/bA est soit nulle, soit celle d'un certain $r \in \mathrm{E}_n(A)$. Autrement dit, on a $a - r \in bA$ avec soit $r = 0$, soit $v(r) < n = v(b)$.

Exercice 6. Anneaux de valuation discrète

Une *valuation discrète* sur un corps K est une application surjective $v : K \to \mathbb{Z} \cup \{+\infty\}$ telle que $v(0) = +\infty$ et pour tous $x, y \in K$, $v(xy) = v(x) + v(y)$ et $v(x+y) \geq \min(v(x), v(y))$; l'ensemble $\{x \in K \mid v(x) \geq 0\}$ est alors un anneau que l'on appelle *anneau de valuation associé à* v. On dit qu'un anneau intègre A est un *anneau de valuation discrète* s'il existe une valuation discrète v sur le corps des fractions de A telle que A est l'anneau de valuation associé à v.

1. Pour $K = \mathbb{Q}$ et p premier, on pose $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ la valuation p-adique. Quel est l'anneau de valuation associé ?

   L'anneau de valuation associé est $\left\{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}^*, (a,b) = 1, p \nmid b\right\}$. Cet anneau est le localisé de $\mathbb{Z}$ par rapport au sous-ensemble multiplicatif $\mathbb{Z} - (p)$.

   Remarque culturelle : en général, si A est un anneau commutatif et $\mathfrak{p}$ en est un idéal premier, le sous-ensemble $S := A - \mathfrak{p} \subseteq A$ est multiplicatif donc on dispose du localisé $S^{-1}A$ que l'on appelle *localisé de* A *en* $\mathfrak{p}$ et on note $A_{\mathfrak{p}}$. Ici, l'anneau de valuation est donc $\mathbb{Z}_{(p)}$.

2. Pour $K = k(X)$, on peut écrire tout polynôme non nul $P(X)$ de manière unique comme $P(X) = X^n P_0(X)$ où le terme constant de $P_0(X)$ est non nul. On pose $v_X(P) = n$ et $v_X(P/Q) = v_X(P) - v_X(Q)$. Quel est l'anneau de valuation associé ?

   L'anneau de valuation associé est $\left\{\frac{P(X)}{Q(X)} \mid P(X) \in k[X], Q(X) \in k[X]^*, (P(X), Q(X)) = 1, X \nmid Q(X)\right\}$. Cet anneau est le localisé de $k[X]$ par rapport au sous-ensemble multiplicatif $k[X] - (X)$; suivant la remarque culturelle faite dans la réponse à la question précédente, c'est le localisé $k[X]_{(X)}$ de $k[X]$ en son idéal maximal (X).

Soit A un anneau de valuation discrète.

3. Montrer que A a un unique idéal maximal $\mathfrak{m}$ (on dit que A est *local*), et que pour tout $n \geq 1$ et tout x_0 avec $v(x_0) = 1$, on a
$$\mathfrak{m}^n = \{x \in K \mid v(x) \geq n\} = (x_0^n).$$

   On commence par remarquer que les inversibles de A sont les éléments de A inversibles dans K dont l'inverse appartient à A, c'est-à-dire les éléments de A de valuation nulle.

   On fixe x_0 avec $v(x_0) = 1$. Soit I un idéal non nul de A. On pose $n = \min(v(I)) \in \mathbb{N}$, de sorte que $x_0^{-n} I$ est un idéal de A et contient un inversible de A (i.e. un élément de valuation nulle). On a donc $x_0^{-n} I = A$ puis $I = (x_0^n)$. On a montré que les seuls idéaux non nuls de A étaient les (x_0^n) pour $n \geq 0$. Comme on a $(x_0^{n+1}) \subsetneq (x_0^n)$ pour $n \geq 0$ (regarder les valuations), on en déduit que A est local d'unique idéal maximal $\mathfrak{m} := (x_0)$. On termine la question en écrivant que pour $n \geq 0$ on a $\mathfrak{m}^n = (x_0^n)$, et $x_0^{-n}\{x \in K \mid v(x) \geq n\} = \{x \in K \mid v(x) \geq 0\} = A$ donc $\{x \in K \mid v(x) \geq n\} = (x_0^n)$.

4. En déduire que A est euclidien.

   On va montrer que pour tout $a \in A$ et tout $b \in A - \{0\}$, il existe un couple (q, r) de A tel que $a = bq + r$ et $r = 0$ ou $v(r) < v(b)$. Soit donc $a \in A$ et $b \in A - \{0\}$. Si $v(a) \geq v(b)$ on a $ab^{-1} \in A$ donc on peut prendre $q = ab^{-1}$ et $r = 0$. Si $v(a) < v(b)$, on peut prendre $q = 0$ et $r = a$. Cela conclut.

5. Quels sont les sous-A-modules du corps des fractions de A ?

   On fixe x_0 avec $v(x_0) = 1$. Soit J un sous-A-module non nul de K. On pose $n = \inf(v(J)) \in \mathbb{Z} \cup \{-\infty\}$.

   Si $n \in \mathbb{Z}$, le sous-A-module $x_0^{-n} J$ de K est inclus dans A donc c'est un idéal de A (on dit que J est un *idéal fractionnaire* ; on peut le multiplier par un élément de A et obtenir un idéal de A). De plus, $x_0^{-n} J$ contient un inversible de A (un élément de valuation nulle) par minimalité de n, donc $x_0^{-n} J = A$ et $J = x_0^n A$.

   Si $n = -\infty$, comme $v(J)$ est stable par $k \mapsto k+1$ (multiplier par x_0) on a $v(J) = \mathbb{Z}$. Ainsi, pour tout $x \in K$ on peut trouver un inversible de A dans $x^{-1} J$, donc $1 \in x^{-1} J$ et $x \in J$. On a donc $J = K$.

   Les sous-A-modules du corps des fractions de A sont donc 0, K et les $x_0^n A$ pour $n \in \mathbb{Z}$ (ce sont tous des idéaux fractionnaires).