

Corrigé du Devoir maison

Soient K un corps et X une indéterminée. On note $A = K[X, X^{-1}]$ le localisé de l'anneau de polynômes $K[X]$ par rapport à la partie multiplicative $\{X^n\}_{n \in \mathbf{N}}$. C'est un sous-anneau du corps $K(X)$ des fractions rationnelles. Notons que si $f \in A \setminus \{0\}$, il existe $v(f) \in \mathbf{Z}$ et $g \in K[X] \setminus XK[X]$ uniques tels que $f = X^{v(f)}g$ (on ne demande pas de prouver ce fait). Bien entendu, $K[X]$ est un sous-anneau de A . De même, $K[X^{-1}] = \{P(X^{-1})\}_{P \in K[X]}$ est lui aussi un sous-anneau de A .

(1) Montrer que $A^\times = K^\times X^{\mathbf{Z}} := \{\lambda X^n\}_{\substack{\lambda \in K^\times \\ n \in \mathbf{Z}}}$.

(2) Montrer que A est principal. Est-il euclidien ?

Munissons $\mathbf{M}_n(A)$ de la relation d'équivalence donnée par

$$M_1 \sim M_2 \Leftrightarrow (\exists U \in \mathbf{GL}_n(K[X])) (\exists V \in \mathbf{GL}_n(K[X^{-1}])) M_2 = UM_1V^{-1}$$

(il n'est pas demandé de justifier qu'il s'agit d'une relation d'équivalence). Le but du problème est de prouver l'énoncé suivant.

Théorème (Dedekind-Weber) Si $n \in \mathbf{N}_{>0}$ et $M \in \mathbf{GL}_n(A)$, il existe des entiers relatifs $d_1 \geq \dots \geq d_n$ uniques tels que

$$(*) \quad M \sim \text{diag}(X^{d_1}, \dots, X^{d_n}).$$

Si en outre M est à coefficients dans $K[X]$, on a $d_n \geq 0$.

(3) Montrer que pour prouver le théorème, il suffit de traiter le cas où M est à coefficients dans $K[X]$, ce qu'on suppose désormais.

(4) Fixons $M \in \mathbf{GL}_n(A)$. Le but de cette question est de montrer l'existence d'une décomposition (*). On procède par récurrence sur $n \in \mathbf{N}_{>0}$.

(a) Traiter le cas $n = 1$.

(b) Montrer qu'il existe $U_0 \in \mathbf{SL}_n(K[X])$ telle que $U_0 M = \begin{pmatrix} f & L \\ 0 & M' \end{pmatrix}$ (écriture par blocs) avec $f \in K[X]$, $L \in \mathbf{M}_{1,n-1}(K[X])$ et $M' \in \mathbf{GL}_{n-1}(A) \cap \mathbf{M}_n(K[X])$.

(c) En déduire qu'il existe des entiers naturels d_1, \dots, d_n tels que $d_2 \geq \dots \geq d_n$ et $f_2, \dots, f_n \in A$ de sorte que M soit équivalente à

$$(♣) \quad \begin{pmatrix} X^{d_1} & f_2 & \cdots & \cdots & f_n \\ 0 & X^{d_2} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & X^{d_n} \end{pmatrix}.$$

(d) Expliquer pourquoi on peut supposer que $f_j \in \langle X^{d_1+1} \rangle \subset K[X]$ et $\deg(f_j) < d_j$ pour tout $j \in \{2, \dots, n\}$.

(e) Expliquer pourquoi parmi toutes les matrices de la forme (♣) équivalentes à M , il en existe une telle que d_1 soit maximal. Prouver que pour une telle matrice, on a $d_1 \geq d_2$.

(f) Conclure.

(5) On veut maintenant prouver l'unicité dans le théorème de Dedekind-Weber. Il s'agit de montrer que si $d_1 \geq \dots \geq d_n$ et $d'_1 \geq \dots \geq d'_n$ sont des suites décroissantes d'entiers

relatifs, $U \in \mathrm{GL}_n(K[X])$ et $V \in \mathrm{GL}_n(K[X^{-1}])$ tels que

$$(\spadesuit) \quad U \operatorname{diag}(X^{d_1}, \dots, X^{d_n}) = \operatorname{diag}(X^{d'_1}, \dots, X^{d'_n})V,$$

alors on a $d_i = d'_i$ pour tout $i \in \{1, \dots, n\}$. Là encore, on raisonne par récurrence sur $n \in \mathbf{N}_{>0}$, le cas $n = 1$ étant trivial (parce que $\mathrm{GL}_1(K[X]) = K^\times = \mathrm{GL}_1(K[X^{-1}])$) : supposons $n \geq 2$.

(a) En traduisant (\spadesuit) coefficient par coefficient, montrer que pour tout $i \in \{1, \dots, n\}$, il existe $\sigma(i) \in \{1, \dots, n\}$ tel que $d_{\sigma(i)} \leq d'_i$. En déduire que $d_n \leq d'_n$, puis que $d_n = d'_n$.

(b) Notons r (resp. s) le plus petit indice $i \in \{1, \dots, n\}$ tel que $d_i = d_n$ (resp. $d'_i = d_n$). Montrer que l'égalité (\spadesuit) implique que $r = s$, et conclure en écrivant U et V par blocs.

Remarque. Mine de rien, ce qui précède fournit une démonstration d'un théorème de géométrie algébrique (dû à Grothendieck, en 1957). On se place sur la droite projective \mathbf{P}_K^1 : c'est la réunion des deux ouverts « affines » $\mathcal{U} = \operatorname{Spec}(K[X])$ et $\mathcal{V} = \operatorname{Spec}(K[T])$ recollés le long des ouverts $\mathcal{U}_0 = \operatorname{Spec}(K[X, X^{-1}])$ et $\mathcal{V}_0 = \operatorname{Spec}(K[T, T^{-1}])$ via l'isomorphisme $K[X, X^{-1}] \rightarrow K[T, T^{-1}]$ défini par $X \mapsto T^{-1}$. Dans ce qui suit, il sera commode d'écrire X^{-1} au lieu de T . Il existe une notion générale de fibré vectoriel sur un « schéma » \mathcal{X} (heuristiquement, un fibré vectoriel est un espace vectoriel qui varie algébriquement au-dessus de \mathcal{X}). Dans le cas $\mathcal{X} = \mathbf{P}_K^1$ qui nous occupe, cela correspond à la donnée d'un $k[X]$ -module libre L_1 et d'un $K[X^{-1}]$ -module L_2 , munis d'une donnée de recollement, c'est-à-dire d'un isomorphisme $A \otimes_{K[X]} L_1 \xrightarrow{\sim} A \otimes_{K[X^{-1}]} L_2$. Après le choix de bases de L_1 et L_2 , cela correspond à la donnée d'un élément de $M \in \mathrm{GL}_n(A)$ (où n est le rang de L_1 sur $K[X]$, qui est aussi le rang de L_2 sur $K[X^{-1}]$). On s'en doute, changer les bases de L_1 et de L_2 remplace M par une matrice équivalente. Il en résulte que classifier les fibrés vectoriels de rang n sur \mathbf{P}_K^1 revient à classifier les éléments de $\mathrm{GL}_n(A)$ modulo équivalence. Le théorème de Dedekind-Weber montre qu'un tel fibré \mathcal{L} se décompose en somme directe de fibrés de rang 1 : on a $\mathcal{L} = \bigoplus_{i=1}^n \mathcal{O}(d_i)$ avec $d_1 \geq \dots \geq d_n$ uniquement déterminés, où $\mathcal{O}(d)$ est le fibré $(K[X], K[X^{-1}], \text{multiplication par } X^d \text{ sur } K[X, X^{-1}])$.

Solution : (1) Si $\lambda \in K^\times$ et $n \in \mathbf{Z}$, on a $(\lambda X^n)^{-1} = \lambda^{-1} X^{-n} \in A$, et donc $\lambda X^n \in A^\times$. Réciproquement, soit $f \in A^\times$. On a $f \neq 0$ et $f^{-1} \neq 0$: on peut écrire $f = X^{v(f)}g$ et $f^{-1} = X^{v(f^{-1})}h$ avec $g, h \in K[X] \setminus XK[X]$. En multipliant, il vient $1 = X^{v(f)+v(f^{-1})}gh$: par unicité, il vient $v(f) + v(f^{-1}) = 0$ (*i.e.* $v(f^{-1}) = -v(f)$) et $gh = 1$. Cela implique en particulier que $g \in K[X]^\times = K^\times$, et montre que $f \in K^\times X^\mathbf{Z}$, et conclut.

(2) • L'anneau A est intègre (c'est un sous-anneau du corps $K(X)$). Soit $I \subset A$ un idéal non nul. Posons $J = I \cap K[X]$: c'est un idéal de $K[X]$. Si $f \in I \setminus \{0\}$, on a $f = X^{v(f)}g$ avec $g \in K[X] \setminus XK[X]$, et $g = X^{-v(f)}f \in I \cap K[X]$, ce qui montre que J est non nul. Comme $K[X]$ est principal, on peut écrire $J = f_0 K[X]$ avec $f_0 \in K[X] \setminus \{0\}$. Comme $f_0 \in J \subset I$, on a bien sûr $\langle f_0 \rangle \subset I$. Réciproquement, soit $f \in I \setminus \{0\}$: comme $X^{-v(f)}f \in J$, il existe $g \in K[X]$ tel que $X^{-v(f)}f = f_0g$, et donc $f = f_0 X^{v(f)}g \in \langle f_0 \rangle$, ce qui montre que $I = \langle f_0 \rangle$ est principal.

• Si $f \in A \setminus \{0\}$, on peut écrire de façon unique $f = X^{v(f)}g$ avec $g \in K[X] \setminus XK[X]$: posons $\varphi(f) = \deg(g) \in \mathbf{N}$. Si $f_1, f_2 \in A \setminus \{0\}$, écrivons $f_1 = X^{v(f_1)}g_1$ et $f_2 = X^{v(f_2)}g_2$ avec $g_1, g_2 \in K[X] \setminus XK[X]$. On a alors $f_1 f_2 = X^{v(f_1)+v(f_2)}g_1 g_2$: par unicité de l'écriture, on a

$$\varphi(f_1 f_2) = \deg(g_1 g_2) = \deg(g_1) + \deg(g_2) = \varphi(f_1) + \varphi(f_2).$$

Par ailleurs, si $f \in A \setminus \{0\}$ et $d \in A \setminus \{0\}$, écrivons $f = X^{v(f)}g$ et $d = X^{v(d)}h$ avec $g, h \in K[X] \setminus XK[X]$. Soit $g = hq_0 + r_0$ avec $q_0, r_0 \in K[X]$ et $\deg(r_0) < \deg(h)$ la division euclidienne de g par h dans $K[X]$. Elle s'écrit $X^{-v(f)}f = X^{-v(d)}dq_0 + r_0$, soit encore $f = qd + r$ avec $q = X^{v(f)-v(d)}q_0 \in A$ et $r = X^{v(f)-v(d)}r_0 \in A$. On a en outre les majorations $\varphi(r) \leq \deg(r_0) < \deg(f) = \varphi(d)$ (remarque : la première inégalité est stricte lorsque r_0 est divisible par X dans $K[X]$). Cela montre que A est euclidien.

(3) Il existe $m \in \mathbf{N}$ tel que $M_1 = X^m M \in \mathbf{M}_n(K[X])$. Comme $X \in A^\times$, on a $M_1 \in \mathbf{GL}_n(A)$. Si on sait qu'il existe $\delta_1 \geq \dots \geq \delta_n \geq 0$ uniques, $U \in \mathbf{GL}_n(K[X])$ et $V \in \mathbf{GL}_n(K[X^{-1}])$ tels que $UM_1V^{-1} = \text{diag}(X^{\delta_1}, \dots, X^{\delta_n})$, on a $UMV^{-1} = \text{diag}(X^{d_1}, \dots, X^{d_n})$ avec $d_k = \delta_k - m$ pour tout $k \in \{1, \dots, n\}$, ce qui prouve l'existence. Si $d'_1 \geq \dots \geq d'_n$ sont des entiers, $U' \in \mathbf{GL}_n(K[X])$ et $V' \in \mathbf{GL}_n(K[X^{-1}])$ sont tels que $U'MV'^{-1} = \text{diag}(X^{d'_1}, \dots, X^{d'_n})$, on a $U'M_1V'^{-1} = \text{diag}(X^{d'_1+m}, \dots, X^{d'_n+m})$: par unicité de $\delta_1 \geq \dots \geq \delta_n$, on a alors $d'_k + m = \delta_k = d_k + m$ i.e. $d'_k = d_k$ pour tout $k \in \{1, \dots, n\}$, ce qui prouve l'unicité.

(4) (a) Si $M \in \mathbf{GL}_1(A) = A^\times = K^\times X^\mathbf{Z}$, on peut écrire $M = (\lambda X^d)$ avec $\lambda \in K^\times$ et $d \in \mathbf{Z}$ (cf question (1)). Il suffit de prendre $U = (\lambda) \in \mathbf{GL}_1(K) \subset \mathbf{GL}_1(K[X])$ et $V = I_1 \in \mathbf{GL}_1(K[X^{-1}])$.

(b) Écrivons $M = (m_{i,j})_{1 \leq i,j \leq n}$, et posons $f = \text{pgcd}_{1 \leq i \leq n} m_{i,1} \in K[X]$ (cela a bien un sens parce que les $m_{i,1}$ ne sont pas tous nuls vu que M est inversible). Écrivons $m_{i,1} = fa_i$ avec $a_i \in K[X]$: on a $\langle a_1, \dots, a_n \rangle = K[X]$. Comme $K[X]$ est principal, on sait (cours), qu'il existe $U_1 \in \mathbf{SL}_n(K[X])$ dont la première colonne est $t(a_1, \dots, a_n)$: si $(\mathbf{e}_1, \dots, \mathbf{e}_n)$ désigne la base canonique de $K(X)^n$, on a donc $U_1^{-1}t(a_1, \dots, a_n) = \mathbf{e}_1$: comme $M\mathbf{e}_1 = f^t(a_1, \dots, a_n)$, on a donc $U_1^{-1}Me_1 = fe_1$, ce qui montre que si $U_0 = U_1^{-1} \in \mathbf{SL}_n(K[X])$, on a $U_0M = \begin{pmatrix} f & L \\ 0 & M' \end{pmatrix}$ avec $L \in \mathbf{M}_{1,n-1}(K[X])$ et $M' \in \mathbf{M}_{n-1}(K[X])$. On a alors $f \det(M') = \det(M) \in A^\times$, donc $\det(M') \in A^\times$, ce qui montre que $M' \in \mathbf{GL}_{n-1}(A)$.

(c) Comme on vient de le voir, on a $f \det(M') = \det(M) \in A^\times$: cela implique que $f \in A^\times = K^\times X^\mathbf{Z}$ (cf question (1)). Écrivons $f = \lambda X^{d_1}$ avec $\lambda \in K^\times$ et $d_1 \in \mathbf{N}$. Par ailleurs, l'hypothèse de récurrence s'applique à $M' \in \mathbf{M}_{n-1}(K[X]) \cap \mathbf{GL}_{n-1}(A)$: il existe $d_2 \geq \dots \geq d_n \geq 0$, $U' \in \mathbf{GL}_{n-1}(K[X])$ et $V' \in \mathbf{GL}_{n-1}(K[X^{-1}])$ tels que

$$U'M'V'^{-1} = \text{diag}(X^{d_2}, \dots, X^{d_n}).$$

Posons alors $U = \begin{pmatrix} \lambda & 0 \\ 0 & U' \end{pmatrix} \in \mathbf{GL}_n(K[X])$ et $V = \begin{pmatrix} 1 & 0 \\ 0 & V' \end{pmatrix} \in \mathbf{GL}_n(K[X^{-1}])$: la matrice UMV^{-1} est de la forme (♣).

(d) Pour $j \in \{2, \dots, n\}$, écrivons $f_i = X^{d_1}g_j + \tilde{f}_j$ avec $g_j \in K[X^{-1}]$ et $\tilde{f}_j \in \langle X^{d_1+1} \rangle \subset K[X]$.

En multipliant la matrice qui précède à droite par $\begin{pmatrix} 1 & -g_2 & \dots & -g_n \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} \in \mathbf{GL}_n(K[X^{-1}])$, on

remplace les f_j par les \tilde{f}_j . De même, soit $\tilde{f}_j = X^{d_j}q_j + r_j$ avec $\deg(r_j) < d_j$ la division euclidienne de \tilde{f}_j par X^{d_j} . Comme $X^{d_1+1} \mid \tilde{f}_j$, on a $X^{d_1+1} \mid r_j$ pour tout $j \in \{2, \dots, n\}$ (on a $r_j = 0$ si $d_j \leq d_1+1$). En multipliant la matrice à gauche par $\begin{pmatrix} 1 & -q_2 & \dots & -q_n \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} \in \mathbf{GL}_n(K[X])$,

on remplace les \tilde{f}_j par les r_j , ce qui conclut.

(e) • Si $U \in \mathbf{GL}_n(K[X])$, on a $\det(U) \in K[X]^\times = K^\times$, d'où $v(\det(U)) = 0$. De même, on a $v(\det(V)) = 0$ pour tout $V \in \mathbf{GL}_n(K[X^{-1}])$: on a $v(\det(UMV^{-1})) = v(\det(M))$ pour tous $U \in \mathbf{GL}_n(K[X])$ et $V \in \mathbf{GL}_n(K[X^{-1}])$. Il en résulte que $d_1 \leq d_1 + \dots + d_n = v(\det(M))$ (parce que $d_2, \dots, d_n \in \mathbf{N}$). Il n'y a qu'un nombre fini de valeurs possibles pour d_1 : on peut trouver $M' \in \mathbf{GL}_n(A)$ équivalente à M , de la forme (♣) et telle que d_1 soit maximal.

- Supposons $d_1 < d_2$. Comme $X^{d_1+1} \mid f_2$, on a $\text{pgcd}(f_2, X^{d_2}) = X^{d'_1}$ avec $d_1 < d'_1 \leq d_2$. Soient $u, v \in K[X]$ tels que $uX^{d_2} + vf_2 = X^{d'_1}$. Écrivons $f = X^{d'_1}g$ avec $g \in K[X]$: on a $uX^{d_2-d'_1} + vg = 1$, donc $\begin{pmatrix} v & u \\ -X^{d_2-d'_1} & g \end{pmatrix} \in \text{SL}_2(K[X])$. On obtient une contradiction avec la maximalité de d_1 en observant que

$$\begin{pmatrix} v & u \\ -X^{d_2-d'_1} & g \end{pmatrix} \begin{pmatrix} X^{d_1} & f_2 \\ 0 & X^{d_2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} X^{d'_1} & X^{d_1}v \\ 0 & X^{d_1+d_2-d'_1} \end{pmatrix}.$$

(f) D'après ce qui précède, il existe une matrice équivalente à M de la forme (♣) telle que $d_1 \geq \dots \geq d_n$ et $f_j \in \langle X^{d_1+1} \rangle$ et $\deg(f_j) < d_j$, et donc $f_j = 0$ pour tout $j \in \{2, \dots, n\}$: on a fini.

(5) (a) Écrivons $U = (u_{i,j})_{1 \leq i,j \leq n}$ et $V = (v_{i,j})_{1 \leq i,j \leq n}$. L'égalité (♠) est équivalente à $X^{d_j}u_{i,j} = X^{d'_i}v_{i,j}$ pour tous $i, j \in \{1, \dots, n\}$. Soit $\sigma(i) \in \{1, \dots, n\}$ tel que $u_{i,\sigma(i)} \neq 0$ (il en existe parce que $U \in \text{GL}_n(K[X])$), ce qui implique $v_{i,\sigma(i)} \neq 0$. Le degré de $X^{d_{\sigma(i)}}i_{i,\sigma(i)}$ est $d_{\sigma(i)} + \deg(u_{i,\sigma(i)})$, et celui de $X^{d'_i}v_{i,\sigma(i)}$ est $\leq d'_i$ (parce que les termes de $v_{i,\sigma(i)}$ sont tous de degrés négatifs ou nuls). Cela implique que $d_{\sigma(i)} \leq d_{\sigma(i)} + \deg(u_{i,\sigma(i)}) \leq d'_i$. En particulier, on a $d_n \leq d_{\sigma(n)} \leq d'_n$. Par symétrie, on a de même $d'_n \leq d_n$, et finalement $d_n = d'_n$.

(b) • De nouveau, écrivons $X^{d_j}u_{i,j} = X^{d'_i}v_{i,j}$. Si $i \geq s$, on a $d'_i = d_n$, ce qui implique que $v_{i,j} = X^{d_j-d_n}u_{i,j} \in \langle X^{d_j-d_n} \rangle$. En particulier, si $j < r$, on a $v_{i,j} \in \langle X \rangle$: comme $v_{i,j} \in K[X^{-1}]$, on a nécessairement $v_{i,j} = 0$, et donc aussi $u_{i,j} = 0$. Cela implique qu'on a une écriture par blocs

$$U = \begin{pmatrix} U_{1,1} & U_{1,2} \\ 0 & U_{2,2} \end{pmatrix}$$

avec $U_{1,1} \in \mathbf{M}_{s-1,r-1}(K[X])$. Si $r-1 > s-1$, les colonnes de $U_{1,1}$ sont liées dans $K(X)^{s-1}$: cela implique que les $r-1$ premières colonnes de U sont liées dans $K(X)^n$, et donc que $\det(U) = 0$, ce qui n'est pas. On a donc nécessairement $r-1 \leq s-1$, i.e. $r \leq s$. La relation (♠) s'écrit aussi

$$U^{-1} \text{diag}(X^{d'_1}, \dots, X^{d'_n}) = \text{diag}(X^{d_1}, \dots, X^{d_n})V^{-1}$$

ce qui échange les rôles des suites $d_1 \geq \dots \geq d_n$ et $d'_1 \geq \dots \geq d'_n$: on a donc aussi $s \leq r$, et finalement $r = s$.

• Si $r = 1$, on a $d_1 = \dots = d_n = d'_1 = \dots = d'_n$ ce qui conclut dans ce cas : supposons maintenant que $r > 1$. On a alors $U_{1,1} \in \mathbf{M}_{r-1}(K[X])$ et $U_{2,2} \in \mathbf{M}_{n-r+1,n-r+1}(K[X])$, et $\det(U) = \det(U_{1,1}) \det(U_{2,2}) \in K^\times$, donc $U_{1,1} \in \text{GL}_{r-1}(K[X])$. De même, cela montre que $V = \begin{pmatrix} V_{1,1} & V_{1,2} \\ 0 & V_{2,2} \end{pmatrix}$ avec $V_{1,1} \in \text{GL}_{r-1}(K[X^{-1}])$. La relation (♠) implique alors que

$$U_{1,1} \text{diag}(X^{d_1}, \dots, X^{d_{r-1}}) = \text{diag}(X^{d'_1}, \dots, X^{d'_{r-1}})V_{1,1}.$$

Comme $d_1 \geq \dots \geq d_{r-1}$ et $d'_1 \geq \dots \geq d'_{r-1}$ et $r-1 < n$, l'hypothèse de récurrence implique que $d_i = d'_i$ pour tout $i \in \{1, \dots, r-1\}$, et donc finalement pour tout $i \in \{1, \dots, n\}$ (parce que $d_r = \dots = d_n = d'_r = \dots = d'_n$).

Remarque. Ce qui précède est fortement inspiré (du moins pour la partie concernant l'existence) de l'article : Hazewinkel, M. & Martin, C. *A short elementary proof of Grothendieck's theorem on algebraic vectorbundles over the projective line*, Journal of Pure and Applied Algebra **25**, p. 207-211 (1982).