MULTIPLICATION DES MATRICES ET VECTEURS DE WITT.

Henri GAUDIER (*) (**)

Dans la théorie classique des invariants, on considère k un corps algébriquement clos de caractéristique 0, et $GL_{n,k}$ le groupe des matrices inversibles $n \times n$ sur k. On s'intéresse aux représentations linéaires de $GL_{n,k}$, c'est à dire aux actions:

$$GL_{n,k} \times V \longrightarrow V,$$

où V est un espace vectoriel sur k, ou bien aux homomorphismes de groupes:

$$\rho : GL_{n,k} \longrightarrow GL(V) = GL_{m,k},$$

qui sont rationnels, et même polynômiaux, c'est à dire que pour tout i', j', $\rho((x_{i,j}))_{i',j'} \in k[x_{i,j}]$. Le morphisme ρ se prolonge alors en un homomorphisme multiplicatif:

$$\rho : M_{n,k} \longrightarrow M_{m,k},$$

qui est lui aussi polynômial.

Le but de ce travail est de construire un anneau, noté $LM_{n,k}$, tel que tout morphisme ρ ayant les propriétés précédentes ait une décomposition:

$$M_{n,k} \to LM_{n,k} \to M_{m,k},$$

où la première flèche est un homomorphisme multiplicatif fixé, et la seconde est un homomorphisme d'anneaux déterminé de façon unique par ρ. La donnée d'une représentation polynômiale de $M_{n,k}$ sera donc équivalente à celle d'un module sur l'anneau $LM_{n,k}$. On peut donc, de ce point de vue considérer $LM_{n,k}$ comme l'algèbre du monoïde $M_{n,k}$ (*cf* [G1]).

Dans le paragraphe 1, on traitera le cas de la caractéristique 0, dans le paragraphe suivant, on s'intéressera à la caractéristique p, et au cas sans caractéristique, en prenant pour V non plus seulement un espace vectoriel, mais plus généralement un module sur l'anneau des vecteurs de Witt.

(*) Département de Mathématiques, Université de Valenciennes, le Mont Houy, F-59313 VALENCIENNES Cedex 9.

(**) Pour ce travail, l'auteur a bénéficié du soutien matériel du P.R.C. Mathématiques-Informatique du C.N.R.S et de l'IRMA de Strasbourg.

1. Le cas de la caractéristique nulle.

Soit $I = M_n(\mathbf{N}) = \{(a_{i,j})_{i,j\in[n]}, \quad a_{i,j} \in \mathbf{N}\}$ on considère alors le k-espace vectoriel $LM_{n,k} = k^I$. Si l'on note $(e_a)_{a\in I}$ sa base (topologique) canonique, on écrira ses éléments sous la forme $\sum_{a\in I} x_a\, e_a$. Considérons alors le morphisme:

$$\begin{aligned} i : M_{n,k} \to & LM_{n,k} \\ (x_{i,j}) \mapsto & \sum_{a\in I}\Big(\prod_{i,j} x_{i,j}^{a_{i,j}}\Big) e_a = \sum_{a\in I} x^a e_a. \end{aligned} \tag{1.1}$$

La proposition suivante est alors immédiate:

Proposition 1 : *Tout morphisme polynômial, ρ de $M_{n,k}$ dans $M_{m,k}$, se factorise de façon unique par une application k-linéaire $\rho' : LM_{n,k} \to M_{m,k}$.*

On peut alors énoncer le résultat principal de ce paragraphe:

Théorème 1 : *Il existe sur $LM_{n,k}$ une unique multiplication telle que:*

a) $LM_{n,k}$ est une k-algèbre,

b) $i(x.y) = i(x).i(y)$,

c) pour tout homomorphisme multiplicatif ρ, l'application ρ', de la proposition précédente est un homomorphisme d'algèbres.

Cette multiplication est donnée par les formules suivantes:

$$x\, e_a . y\, e_b = \sum_{c\in I} n_{a,b,c} xy\, e_c, \tag{1.2}$$

avec

$$n_{a,b,c} = \sum_{\nu} \prod_{i,j\in[n]} (\!(\nu_{i,j,1}, \ldots, \nu_{i,j,n})\!), \tag{1.3}$$

où la somme est étendue aux

$$\nu = (\nu_{i,j,k})_{i,j,k\in[n]}, \qquad \nu_{i,j,k} \in \mathbf{N}, \tag{1.4}$$

tels que:

$$\sum_j \nu_{i,j,k} = a_{i,k}, \tag{1.5}$$

$$\sum_i \nu_{i,j,k} = b_{k,j}, \tag{1.6}$$

$$\sum_k \nu_{i,j,k} = c_{i,j}. \tag{1.7}$$

On a noté $(\!(t_1, \ldots, t_n)\!)$ le coefficient multinômial $\binom{t_1+\cdots+t_n}{t_1,\ldots,t_n}$.

Les conditions (1.5) à (1.7) peuvent se représenter de la façon suivante: si l'on représente $(\nu_{i,j,k})$ comme un tableau tridimensionnel d'entiers (fig 1), la condition (1.5) dit que si l'on projette le tableau ν sur le plan de coordonnées i, k en additionnant les coefficients de ν qui ont même projection, on obtient la matrice a; la condition (1.6) dit que la projection sur le plan j, k donne la transposée de b, et par (1.7), c est obtenu par projection sur le plan i, j.

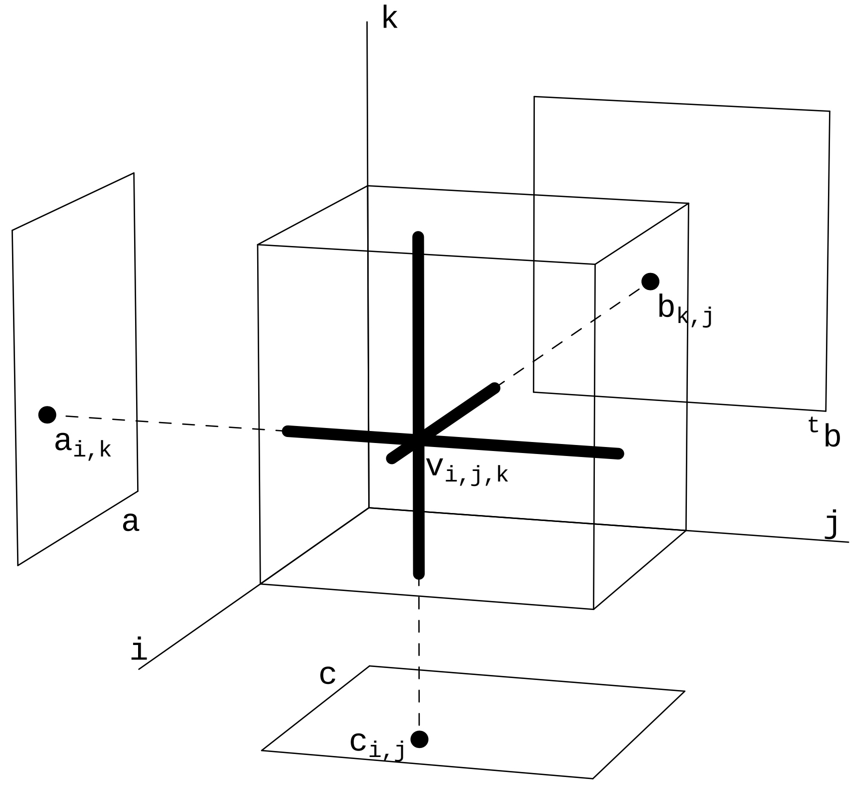
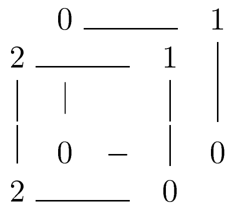


Figure 1

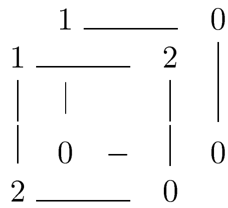
Exemple. — Calculons le produit

$$e^{\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}} . e^{\begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix}} .$$

On vérifie que les seuls ν possibles sont les suivants:



et



D'où l'on obtient:

$$e_{\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}} . e_{\begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix}} = 6\, e_{\begin{pmatrix} 0 & 1 \\ 4 & 1 \end{pmatrix}} + 3\, e_{\begin{pmatrix} 1 & 0 \\ 3 & 2 \end{pmatrix}} .$$

Remarques. — Il est facile de voir que beaucoup de coefficients $n_{a,b,c}$ sont nuls: pour avoir un coefficient non nul on doit évidemment avoir:

$$\sum_{i,k} a_{i,k} = \sum_{k,j} b_{k,j} = \sum_{i,j} c_{i,j} .$$

Plus précisément on doit même avoir:

$$\begin{aligned} \sum_i a_{i,k} &= \sum_j b_{k,j} && \text{pour tout} \quad k, \\ \sum_k a_{i,k} &= \sum_j c_{i,j} && \text{pour tout} \quad i, \\ \sum_k b_{k,j} &= \sum_i c_{i,j} && \text{pour tout} \quad j. \end{aligned}$$

Rappelons d'autre part que la théorie classique des invariants dit que toute représentation linéaire de $GL_{n,k}$ est semi-simple, il en résulte que l'anneau $LM_{n,k}$ se décompose en un produit d'anneaux isomorphes à des anneaux de matrices. La remarque ci-dessus permet de commencer cette décomposition.

Remarquons enfin que l'élément unité de l'anneau $LM_{n,k}$ est:

$$i \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} = \sum_d e_d ,$$

où la somme est étendue à toute les matrices diagonales d.

2. Le cas de la caractéristique p, et le cas sans caractéristique.

Commençons par nous placer en caractéristique p. Le corps k, est supposé algébriquement clos ou parfait de caractéristique p, et au lieu de regarder les représentations de $GL_{n,k}$ dans un espace vectoriel sur k, nous allons généraliser en regardant les représentations de $GL_{n,k}$ dans un module sur un anneau "algébrique" sur k. On démontre [G1] que sous certaines hypothèses peu restrictives, cela revient à regarder les représentations polynômiales de $GL_{n,k}$ dans un module sur l'anneau des p-vecteurs de Witt. Comme dans le cas de la caractéristique 0, on doit alors construire une W-algèbre WM_n et un morphisme multiplicatif $i : M_{n,k} \to WM_n$, tel que tout morphisme multiplicatif $\rho : M_{n,k} \to A$ où A est une W-algèbre, admette une décomposition unique $\rho = \rho'.i$, où $\rho' : WM_n \to A$ est un homomorphisme de W-algèbres.

Pour éviter des redites et parce que les constructions en caractéristique p, et sans caractéristique sont très semblables, nous allons tout de suite nous placer dans ce dernier cas et construire l'algèbre $\mathbf{W}M_n$ sur l'anneau $\mathbf{W}$ des vecteurs de Witt au dessus de l'anneau des entiers.

L'anneau des vecteurs de Witt. — Donnons tout d'abord une présentation très succinte des vecteurs de Witt. Pour une description plus précise, le lecteur pourra se reporter à [G2] ou à [DS].

Si R est un anneau commutatif avec unité, l'anneau $\mathbf{W}$ est défini par:

$$\mathbf{W}(R) = R^{\mathbf{N}} = \{(a_1, \ldots, a_n, \ldots) \quad a_n \in R\}.$$

L'addition et la multiplication dans $\mathbf{W}(R)$ sont telles que pour tout entier n, le morphisme

$$\begin{aligned} w_n : \mathbf{W}(R) &\to R \\ (a_1, \ldots, a_n, \ldots) &\mapsto \sum_{d|n} d\, a_d^{n/d}, \end{aligned}$$

est un homomorphisme d'anneaux. On démontre que les composantes de la somme et du produit de deux vecteurs de Witt s'expriment comme des polynômes à coefficients entiers en les composantes de ces deux vecteurs.

Si $a \in R$, on pose $\tau(a) = (a, 0, 0, \ldots) \in \mathbf{W}(R)$.On a alors:

$$\tau(a).(a_1, \ldots, a_n, \ldots) = (aa_1, a^2 a_2, \ldots, a^n a_n, \ldots).$$

On note V_m l'homomorphisme de groupe $\mathbf{W} \to \mathbf{W}$ tel que:

$$V_m(a_1, \ldots, a_n, \ldots) = (\underbrace{0, \ldots, 0}_{n-1 \text{ fois}}, a_1, \underbrace{0, \ldots, 0}_{n-1 \text{ fois}}, a_2, 0 \ldots).$$

On note F_m l'unique homomorphisme d'anneaux $\mathbf{W} \to \mathbf{W}$ tel que $F_m(\tau(a)) = \tau(a^m)$.

Enfin si $i_1, \ldots, i_n \in \mathbf{Q}_{\geq}$ i.e. $i_k \geq 0$, on note ${}^*(\!(i_1, \ldots, i_n)\!)$ le vecteur de Witt tel que:

$$\begin{aligned} w_m({}^*(\!(i_1, \ldots, i_n)\!)) &= (\!(mi_1, \ldots, mi_n)\!) \quad \text{si} \quad mi_1, \ldots, mi_n \in \mathbf{N}, \\ &= 0 \qquad\qquad\qquad\qquad \text{sinon.} \end{aligned}$$

On montre alors [G2] que si $i_1 + \cdots + i_n \in \mathbf{N}$, si $l \,|\, (i_1 + \cdots + i_n)$ et $pgcd(l, i_1, \ldots, i_n) = 1$, alors ${}^*(\!(i_1, \ldots, i_n)\!)/l \in \mathbf{W}(\mathbf{Z})$.

Si p est un nombre premier, l'anneau des p-vecteurs de Witt est l'anneau quotient de $\mathbf{W}$ défini par la projection :

$$\begin{aligned} \pi : \mathbf{W} &\to W \\ (a_1, \ldots, a_n, \ldots) &\mapsto (a_1, a_p, \ldots, a_{p^n}, \ldots). \end{aligned}$$

On notera V et F les images par π des homomorphismes V_p et F_p de $\mathbf{W}$, et par ${}^p(\!(i_1, \ldots, i_n)\!)$ celle de ${}^*(\!(i_1, \ldots, i_n)\!)$.

Construction de $\mathbf{W}M_n$. — Soit $J = M_n(\mathbf{Q}_{\geq})$, si $a = (a_{i,j}) \in J$, on pose $d(a) = ppcm$(dénominateur $a_{i,j}$). On considère alors le $\mathbf{W}$-module:

$$\overline{\mathbf{W}M}_n = \mathbf{W}^J = \Big\{ \sum_{a \in J} x_a \overline{e}_a \Big\},$$

que l'on munit de la multiplication:

$$x\, \overline{e}_a . y\, \overline{e}_b = \sum_{c \in J} n_{a,b,c} xy\, \overline{e}_c, \tag{2.1}$$

avec

$$n_{a,b,c} = \sum_{\nu} \prod_{i,j \in [n]} {}^*(\!(\nu_{i,j,1}, \ldots, \nu_{i,j,n})\!), \tag{2.2}$$

où la somme est étendue aux

$$\nu = (\nu_{i,j,k})_{i,j,k \in [n]}, \qquad \nu_{i,j,k} \in \mathbf{Q}_{\geq}, \tag{2.3}$$

vérifiant les relations (1.5) à (1.7).

Proposition 2 : $\overline{\mathbf{W}M}_n$ *est une algèbre associative sans élément unité, et*

$$\varepsilon = \sum_{a \text{ diagonale}} {}^*(\!(0, 1/d(a))\!)\overline{e}_a$$

est un idempotent central.

Considérons maintenant $\mathbf{W}M_n$ une autre copie de $\mathbf{W}^J$ de base $(e_a)_{a\in J}$, et le morphisme:

$$\begin{aligned} \varphi : \mathbf{W}M_n &\to \overline{\mathbf{W}M}_n \\ w\, e_a &\mapsto \frac{1}{d(a)} V_{d(a)}(w)\, \overline{e}_a. \end{aligned}$$

Théorème 2 : *1) L'homomorphisme φ est injectif et a pour image $\varepsilon\overline{\mathbf{W}M}_n$, il donne donc à $\mathbf{W}M_n$ une structure de $\mathbf{W}$-algèbre avec unité.*

2) Le morphisme :

$$\begin{aligned} j : M_n &\to \mathbf{W}M_n \\ (x_{i,j}) &\mapsto \sum_{a\in J} \tau\big(x^{d(a)a}\big) e_a, \end{aligned}$$

est compatible avec la multiplication.

Remarques. — 1) Dans l'algèbre $\overline{\mathbf{W}M}_n$, la multiplication est définie par des polynômes à coefficients dans $\mathbf{Q}$, donc $\overline{\mathbf{W}M}_n(R)$ n'a de sens que si R est une $\mathbf{Q}$-algèbre. Par contre dans $\mathbf{W}M_n$ la multiplication est définie par des polynômes à coefficients entiers et $\mathbf{W}M_n$ a donc un sens pour tout anneau R. On peut d'ailleurs donner la formule de la multiplication:

$$xe_a.ye_b = \sum_c \sum_\nu V_{d(\nu)/d(c)} \Big[\frac{d(c)}{d(\nu)} \prod_{i,j} {}^*(\!(d(\nu)\nu_{i,j,1}, \ldots, d(\nu)\nu_{i,j,n})\!) F_{d(\nu)/d(a)}(x)\, F_{d(\nu)/d(b)}(y) \Big] e_c.$$

2) Le morphisme multiplicatif $\varphi.j : M_n \to \overline{\mathbf{W}M}_n$ est donné par:

$$\varphi.j(x) = \sum_a {}^*(\!(0, 1/d(a))\!)\tau(x^a)\overline{e}_a.$$

Il est clair alors que tout $\mathbf{W}M_n$-module donne par l'intermédiaire du morphisme j une représentation polynômiale à coefficients entiers de M_n

dans un $\mathbf{W}$-module. Je ne sais pas encore si l'on obtient ainsi toutes les représentations.

Exemple. — Calculons le produit

$$\overline{e}_{\begin{pmatrix}0&1\\2&3\end{pmatrix}}.\overline{e}_{\begin{pmatrix}2&0\\2&2\end{pmatrix}}.$$

On obtiendra cette fois ci une infinité de tableaux ν qui seront de la forme:

$$\begin{array}{cccccc} & & \alpha & \underline{\qquad\qquad} & & 1-\alpha \\ 2-\alpha & \underline{\qquad} & & 1+\alpha & & | \\ | & | & & | & & | \\ | & 0 & - & -|- & & -0 \\ 2 & \underline{\qquad} & & 0 & & \end{array}\ .$$

Ce qui donne:

$$\begin{aligned}
\overline{e}_{\begin{pmatrix}0&1\\2&3\end{pmatrix}}.\overline{e}_{\begin{pmatrix}2&0\\2&2\end{pmatrix}} &= \sum_{\alpha\in[0,1]} {}^*(\!(2,2-\alpha)\!)\,\overline{e}_{\begin{pmatrix}\alpha&1-\alpha\\4-\alpha&1+\alpha\end{pmatrix}}, \\
&= {}^*(\!(2,2)\!)\,\overline{e}_{\begin{pmatrix}0&1\\4&1\end{pmatrix}} + {}^*(\!(2,1)\!)\,\overline{e}_{\begin{pmatrix}1&0\\3&2\end{pmatrix}} + {}^*(\!(2,3/2)\!)\overline{e}_{\begin{pmatrix}1/2&1/2\\7/2&3/2\end{pmatrix}} \\
&\quad + {}^*(\!(2,5/3)\!)\overline{e}_{\begin{pmatrix}1/3&2/3\\11/3&4/3\end{pmatrix}} + {}^*(\!(2,4/3)\!)\overline{e}_{\begin{pmatrix}2/3&1/3\\10/3&5/3\end{pmatrix}} + \cdots
\end{aligned}$$

Dans l'algèbre $\mathbf{W}M_n$ on a:

$$\begin{aligned}
x\,e_{\begin{pmatrix}0&1\\2&3\end{pmatrix}}.y\,e_{\begin{pmatrix}2&0\\2&2\end{pmatrix}} &= \sum_{\alpha\in[0,1]} {}^*(\!(d(\alpha)2, d(\alpha)(2-\alpha))\!)\,F_{d(\alpha)}(xy)\,e_{\begin{pmatrix}\alpha&1-\alpha\\4-\alpha&1+\alpha\end{pmatrix}}, \\
&= {}^*(\!(2,2)\!)\,xy\,e_{\begin{pmatrix}0&1\\4&1\end{pmatrix}} + {}^*(\!(2,1)\!)\,xy\,e_{\begin{pmatrix}1&0\\3&2\end{pmatrix}} \\
&\quad + {}^*(\!(4,3)\!)\,F_2(xy)\,e_{\begin{pmatrix}1/2&1/2\\7/2&3/2\end{pmatrix}} + {}^*(\!(6,5)\!)\,F_3(xy)\,e_{\begin{pmatrix}1/3&2/3\\11/3&4/3\end{pmatrix}} \\
&\quad + {}^*(\!(6,4)\!)\,F_3(xy)\,e_{\begin{pmatrix}2/3&1/3\\10/3&5/3\end{pmatrix}} + \cdots
\end{aligned}$$

Le cas de la caractéristique p. — On construit des anneaux $\overline{WM}_n$, WM_n et le morphisme j_p de la même façon que $\overline{\mathbf{W}M}_n$, $\mathbf{W}M_n$ et j en remplaçant simplement $\mathbf{Q}_{\geq}$ par $\mathbf{N}[p^{-1}]$, les coefficients ${}^*(\!(\ldots)\!)$ sont alors remplacés par leurs projections ${}^p(\!(\ldots)\!)$. On obtient alors:

Théorème 3 : *La multiplication dans WM_n est à coefficients dans $\mathbf{F}_p$, et il y a équivalence entre les représentations W-linéaires de M_n et les modules sur la W-algèbre WM_n, l'équivalence se faisant à l'aide du morphisme j_p.*

Références:

[DS] A.W.M. DRESS, Ch. SIEBENEICHER. — *The Burnside ring of profinite groups and the Witt vector construction.* Advances in Math., **70**, (1988), 87-132.

[G1] H. GAUDIER. — *Groupes libres et algèbres de groupes en Géométrie algébrique.* Manuscr. Math., **25**, (1978), 79-96.

[G2] H. GAUDIER. — *Relèvement des coefficients binômiaux dans les vecteurs de Witt.* Séminaire Lotharingien de Combinatoire 18e session. Publ. Math. IRMA Strasbourg n° 358/S18, (1988), 93-108.
http://www.mat.univie.ac.at/~slc/opapers/s18gaudier.html