Séminaire Dubreil.
Algèbre et théorie
des nombres

Paul M. Cohn

Numérateurs et dénominateurs dans le corps de fractions d'un semifir

Séminaire Dubreil. Algèbre et théorie des nombres, tome 28, nº 1 (1974-1975), exp. nº 28, p. 1-7

<http://www.numdam.org/item?id=SD_1974-1975__28_1_A22_0>

© Séminaire Dubreil. Algèbre et théorie des nombres
(Secrétariat mathématique, Paris), 1974-1975, tous droits réservés.

L'accès aux archives de la collection « Séminaire Dubreil. Algèbre et théorie des nombres » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

Numdam
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire P. DUBREIL
(Algèbre)
28e année, 1974/75, n° 28, 7 p.

10 juin 1975

NUMÉRATEURS ET DÉNOMINATEURS DANS LE CORPS DE FRACTIONS D'UN SEMIFIR

par Paul M. COHN

1. Tout le monde sait ce qu'est un numérateur et un dénominateur. Et pourtant, il y a des subtilités même dans le cas commutatif. Etant donné un domaine d'intégrité (commutatif) R, il possède un corps de fractions $F(R)$, dont tout élément peut s'exprimer sous la forme

$$u = a/b . \tag{1}$$

Ici a est le numérateur, b le dénominateur de cette expression pour u. La question est la suivante : peut-on trouver une expression (1) pour u qui soit distinguée de quelque façon, c'est-à-dire, y-a-t'il une forme normale ?

Pour $R = \mathbb{Z}$, la réponse est affirmative ; on peut écrire $u = a/b$, où $(a,b)=1$ et $b > 0$, et sous ces conditions, a, b sont uniques. Egalement, on a une forme normale pour $k[X]$ (k corps), et quand on regarde de près, on voit que, pour tout anneau factoriel, on peut trouver une forme normale en prenant un représentant pour chaque irréductible. Cette forme normale possède en plus la propriété agréable de fournir des dénominateurs universels. Etant donné un homomorphisme dans un corps

$$\lambda : R \longrightarrow K ,$$

$u\lambda$ est défini dans K si, et seulement si, $b\lambda \neq 0$. Car si $b\lambda = 0$, alors $u \longmapsto \infty$, et si $b\lambda = a\lambda = 0$, il n'y a aucun choix de dénominateur pour u qui éviterait cette situation.

Par contre, dans l'anneau d'un quadrique $xt = yz$ (anneau non factoriel canonique), on a $x/y = z/t$. Quand on considère l'homomorphisme $R \longrightarrow k(z , t)$, qui consiste à poser $x = y = 0$, on trouve quand même que z/t est définie.

2. Notre but est d'examiner de près la situation non commutative. Je vais me limiter aux semifirs, pour lesquels il y a un bon corps de fractions. Rappelons rapidement les définitions : un semifir est un anneau dont tout idéal à gauche, ou à droite, de type fini, est libre, de rang unique. D'ailleurs, nous n'aurons pas besoin de retenir cette définition, mais seulement que la classe des semifirs comprend des algèbres libres et les produits libres de corps (même gauche). Bien sûr, nous devons nous rappeler qu'un semifir R a un corps de fractions, dont les éléments se construisent comme composantes des solutions des équations

$$Au = a , \tag{2}$$

où a est une colonne dans R, et A une matrice pleine sur R, c'est-à-dire

qu'on ne peut pas écrire $A = PQ$, où P est $n \times r$, Q est $r \times n$ et $r < n$. Rappelons la règle de Cramer dans le cas commutatif : si on pose $A = (a_1, \ldots, a_n)$, $A_1 = (a_1, a_2, \ldots, a_n)$, alors la première composante u_1 de u est donnée par la formule

$$u_1 = \det A_1 / \det A .$$

Dans le cas général, nous n'avons pas de déterminant, mais il existe quand même une règle de Cramer ; elle dit : u_1 est inversible si, et seulement si, A_1 est pleine. La démonstration est simple :

$$A_1 = (Au_1, Ae_2, \ldots, Ae_n) = A\begin{pmatrix} u_1 & 0 \\ u' & I \end{pmatrix} = A\begin{pmatrix} u_1 & 0 \\ 0 & I \end{pmatrix}\begin{pmatrix} 1 & 0 \\ u' & I \end{pmatrix} .$$

Ici u' est la colonne u "décapitée".

Notre tâche sera la comparaison des différentes équations (2) qui définissent u_1. Or le système (2) est entièrement défini par sa matrice (A, a) qui est $n \times (n+1)$. Pour décrire de telles matrices, il nous faut une petite digression.

3. Tout module M de présentation finie sur un anneau R peut s'écrire

$$(3) \qquad {}^nR \xrightarrow{\alpha} {}^mR \longrightarrow M \longrightarrow 0 .$$

Ici ${}^nR$ est le module libre de rang n, conçu comme module de colonnes, et α est réalisé par une matrice $m \times n$ A. Quand R est un semifir, $\operatorname{Im}\alpha$ est libre, de rang $\leqslant n$, donc on peut alors supposer que α soit injectif, c'est-à-dire A n'est pas diviseur de zéro à gauche. Dans ce cas là, $\chi(M) = m - n$ est un invariant de M, et nous dirons que M est complètement présenté par A.

Si on pose $M^* = \operatorname{Hom}_R(M, R)$, et dualise (3), on obtient

$$0 \longrightarrow M^* \longrightarrow R^m \longrightarrow R^n \longrightarrow \operatorname{Ext}^1_R(M, R) \longrightarrow 0$$

(où R^m, etc. est un module libre de lignes). Nous voyons que A n'est pas diviseur de zéro à droite si, et seulement si, $M^* = 0$, c'est-à-dire M est un module lié. Le rang intérieur d'une matrice $m \times n$, A est le plus petit entier r tel qu'on ait $A = PQ$, où P est $m \times r$ et Q est $r \times n$. Par exemple, une matrice $n \times n$ est de rang intérieur n si, et seulement si, elle est pleine.

Définition. - Un module M sur un semifir R est plein s'il est lié, à présentation

$$0 \longrightarrow {}^nR \longrightarrow {}^mR \longrightarrow M \longrightarrow 0 ,$$

et la matrice de M a un rang intérieur $\min(m, n)$.

Il est facile de trouver une description invariante.

THÉORÈME 1. - Soient R un semifir, M un module de présentation finie. Alors H est plein, si, et seulement si, une des conditions suivantes est satisfaite :

(a) M est lié, et $\chi(M') \geqslant 0$ pour tout sous-module M' de M ;

(b) $\chi(M'') \leqslant 0$ pour tout module quotient M'' de M .

Il suffit de noter que (b) entraîne que M est lié.

Un module plein est appelé positif, négatif ou de torsion selon que $\chi(M)$ est $\geqslant 0$, $\leqslant 0$ ou $= 0$. Cette définition de module de torsion s'accorde avec celle donnée dans [1]. Les sous-catégories, pleines de Mod_R qui correspondent à ces classes sont désignées par Pos_R , Neg_R et Tor_R . Il est évident qu'on a

$$\mathrm{Tor}_R = \mathrm{Pos}_R \cap \mathrm{Neg}_R .$$

De plus, il y a une dualité entre Pos_R et ${}_R\mathrm{Neg}$, définie par $\mathrm{Ext}^1_R(- , R)$ (cf. [1], chap. 5, et [2]).

Nous aurons besoin de conditions sur des matrices A , A' pour qu'elles définissent des modules isomorphes. A l'aide du lemme de Schanuel, on constate que A , A' (toutes les deux non-diviseurs de zéro à gauche) définissent des modules isomorphes si, et seulement si, ils sont "stablement associées" c'est-à-dire il existe des matrices P , Q inversibles et des matrices unités telles que

$$P\begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix} Q = \begin{pmatrix} A' & 0 \\ 0 & I \end{pmatrix} .$$

Il y a une autre condition, valable dans les semifirs (même dans les anneaux faiblement finis, c'est-à-dire qui vérifient la condition suivante : $UV=I \Longrightarrow VU=I$ pour toutes matrices U , V) : Deux matrices A , A' définissent des modules isomorphes si, et seulement si, il y a une relation comaximale

$$AB' = BA' .$$

Ceci veut dire : toute colonne est combinaison linéaire à droite des colonnes de (A , B) , et toute ligne est combinaison linéaire à gauche des lignes de $\begin{pmatrix} B' \\ A' \end{pmatrix}$.

4. Soit R un semifir, $U = U(R)$, son corps universel de fractions. Tout élément $u_1 \in U$ satisfait à une équation

$$Au = a , \quad A \text{ pleine } n \times n . \tag{4}$$

Plus généralement, on peut prendre $a \in {}^mR$, $A \in {}^mR^n$ (matrice $m \times n$) avec $\mathrm{rg}\, A = n$ (donc $n \leqslant m$). En partant de cette forme plus générale, on retombe sur sur le cas précédent en choisissant n lignes de A qui constituent une matrice pleine.

On appelle n l'ordre du système, et le minimum des valeurs de l'ordre est la profondeur de u_1 . Par exemple, u_1 est de profondeur 1 si, et seulement si, on a $u_1 = a_1^{-1} a$ ($a , a_1 \in R$, $a \notin a_1 R$) ; ce cas, à peu près trivial, sera exclu dans la suite. Nous voyons que u_1 est défini par la matrice

$$A^* = (a , a_1 , \ldots , a_n) , \quad m \times (n+1) \text{ de rang } n .$$

Il s'agit de trouver comment on peut faire varier A^* sans affecter u_1 . Nous avons les opérations suivantes :

La transformation λ , qui consiste à remplacer A^* par PA^* , $P \in {}^{\ell}R^{m}$, rg $P = m$. Par la loi de nullité, $n \geq rg(PA) \geq rg\ A - m = n - m - m = n$, donc rg $PA = n$, et on a encore (4).

La transformation inverse est note λ' . S'il n'existe pas d'opération inverse (sauf quand P est inversible), on appelle A^* réduit à gauche. Notons que λ augmente m , λ' le diminue, mais ne le rend pas inférieur à n , et si la valeur n est atteinte par m , elle reste constante par application de λ' .

On a une deuxième opération :

La transformation ρ qui consiste à remplacer A^* par $A^* Q$, où

$$Q = \begin{pmatrix} I_r & 0 \\ pq & Q_1 \end{pmatrix} \qquad Q \in {}^{n+1}R^{s+1} , \quad rg\ Q = s + 1 .$$

Contrairement à ce que fait λ , ρ change l'ordre du système en s , et les conditions sur Q assurent que $s \leq n$. L'opération inverse, ρ' , consiste à diviser par Q à droite. Si aucune opération ρ' n'est possible, A^* s'appelle réduit à droite. Cela veut dire : qu'aucune transformation ρ n'abaisse l'ordre, et la seule transformation ρ' qui n'augmente par l'ordre correspond à une matrice inversible. Une matrice réduite à droite et à gauche est appelée réduite.

Passons maintenant à la réduction des systèmes. D'abord, deux lemmes sur les matrices dans un semifir.

LEMME 1. - Soit R un semifir, $P \in {}^{m}R^{r}$, $Q \in {}^{r}R^{n}$; si $PQ = 0$, alors il existe $T \in GL_r(R)$ tel que $PT^{-1} = (P_1\ 0)$, $TQ = \begin{pmatrix} 0 \\ Q_1 \end{pmatrix}$ (où dans les seconds membres sont des blocs de matrices dont le nombre des lignes et colonnes sont tels que l'opération $(PT^{-1})TQ$) soit possible.

Cela est presque une conséquence de la définition même d'un semifir (cf. [1], ch. ch. 1) : Les colonnes de P engendrent un sous-module de type fini de ${}^{m}R$ qui doit être libre, et on en prend une base pour composer P_1 .

LEMME 2. - Dans un semifir, si on a

$$PQ = \begin{pmatrix} A_1 & 0 \\ A_3 & A_4 \end{pmatrix}$$

alors il existe une matrice T inversible telle que

$$PT^{-1} = \begin{pmatrix} P_1 & 0 \\ P_3 & P_4 \end{pmatrix} \qquad TQ = \begin{pmatrix} Q_1 & 0 \\ Q_3 & Q_4 \end{pmatrix} .$$

Démonstration. - Si on pose $P = \begin{pmatrix} P' \\ P'' \end{pmatrix}$, $Q = (Q'\ Q'')$, alors $P'\ Q'' = 0$, donc on peut trouver T tel que $P'\ T^{-1} = (P_1\ 0)$, $TQ'' = \begin{pmatrix} 0 \\ Q_4 \end{pmatrix}$: Si on écrit

$$P''\ T^{-1} = (P_3\ P_4) \ ; \quad TQ' = \begin{pmatrix} Q_1 \\ Q_3 \end{pmatrix} ,$$

on obtient la forme voulue.

Supposons qu'on ait deux systèmes

$$Au = a\ , \qquad A \in {}^{m}R^{n} \quad \operatorname{rg} A = n\ ,$$

$$Bv = b\ , \qquad B \in {}^{v}R^{s} \quad \operatorname{rg} B = s\ .$$

L'équation de $u_1 - v_1$ s'écrit

$$\begin{pmatrix} A & a_1 & 0 \\ 0 & & B \end{pmatrix} \begin{pmatrix} u_1 - v_1 \\ u' \\ v \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}.$$

Ici a_1 est la première colonne de A_1 et $u = \binom{u_1}{u'}$. Dire que $u_1 = v_1$ équivaut à dire que la matrice

$$\left(\begin{array}{c|c} A & a0 \\ \hline b_1 \quad 0 & B_1 \end{array}\right) \text{ est de rang } < n + s \qquad (B_1 = (b\ ,\ b_2\ ,\ldots,\ b_s))\ .$$

Donc (lemme 2), on obtient

$$\left(\begin{array}{c|c} A & a0 \\ \hline b_1 \quad 0 & B_1 \end{array}\right) = \begin{pmatrix} P_1 & 0 \\ P_3 & P_4 \end{pmatrix} \begin{pmatrix} Q_1 & 0 \\ Q_3 & Q_4 \end{pmatrix} \quad \text{où} \quad \begin{array}{ll} A = P_1\, Q_1' & B' = P_4\, Q_4 \\ Q_1 = (q\ Q_1') & B = (b_1\ B') \end{array}\ .$$

Après de léger calculs (en appliquant λ' à A^*, ρ' à B^*) on trouve

$$\left(\begin{array}{c|c} A & a0 \\ \hline b_1 \quad 0 & B_1 \end{array}\right) = \begin{pmatrix} I & 0 \\ P & B' \end{pmatrix} \begin{pmatrix} A & a & 0 \\ 0-Q & 0 & I \end{pmatrix}\ . \tag{5}$$

Donc on a

$$PA^* = B^*\, Q \quad \text{où} \quad Q = \begin{pmatrix} I_2 & 0 \\ qq_1 & Q' \end{pmatrix}\ . \tag{6}$$

Si B^* est réduit à droite, $\operatorname{rg} Q = s$, et alors $s \leqslant n$ (sinon, on pourrait réduire B^*). Pareillement, si A^* est réduit à gauche, on a $m \leqslant r$. Donc on aboutit au résultat suivant :

THÉORÈME 2. - Soit R un semifir à corps de fractions U. Soit $u_1 \in U$, et soit $A^* = (aA)$ un système pour u_1.

(i) Si A^* est réduit à gauche, elle est de la forme $n \times n + 1$,

(ii) Si A^* est réduit à droite, son ordre minimal est égal à la profondeur de u_1.

(iii) Si A^* est réduit à gauche, et B^* un autre système pour u_1, réduit à droite, il y a une équation

$$PA^* = B^*\, Q\ . \tag{7}$$

(iv) Si A^*, B^* sont deux systèmes réduits pour u_1, ils ont même ordre et (7) peut être prise comme relation comaximale.

On peut interpréter la dernière assertion comme suit : Soit M le module à gauche défini par A^*, alors M est plein, en effet il est de caractéristique 1. La transformation $A^* \longrightarrow B^*$, exprimée par (7), consiste en un changement de relations définissantes, suivi d'un changement de générateur qui laisse fixe deux élé-

ments correspondant aux deux premières colonnes de A^* . Donc u_1 est spécifié par un module positif de caractéristique 1 , avec une paire d'éléments distingués. Si on désigne les générateurs par e_0 , e_1 , ... , e_n il y a une relation unique (sur U) à un multiple scalaire près :

$$\lambda_0 e_0 + \lambda_1 e_1 + \ldots + \lambda_n e_n = 0 ,$$

et $u_1 = - \lambda_0^{-1} \lambda_1$.

5. Quoique les résultats obtenus soient assez explicites, il n'est pas facile de les exploiter. Un cas important est celui des semifirs "conservateurs", c'est-à-dire un semifir R qui contient un corps K , et qui est contenu dans un semifir R(t) contenant K(t) . Ici t est une indéterminée centrale dans K . Pour un tel semifir R , on peut montrer que : Si A est une matrice (rectangulaire) sur R , non-diviseur de zéro, alors l'anneau propre ("eigenring") de A est algébrique (à droite) sur K .

Ici l'anneau propre de $A \in {}^mR^n$ est $\mathrm{End}({}^mR/A({}^nR))$, ou si l'on veut, End(M) pour un module M complètement présenté par A . Le résultat est analogue au cas spécial démontré dans [1] (p. 170).

L'hypothèse sur R est satisfaite pour $R = K_k\langle X\rangle \subset K(t)_{k(t)}\langle X\rangle$. Soit R un semifir conservateur, et soit U son corps de fractions. Etant donné $x \in R$, x non algébrique sur K , et $y \in U$ tel que $xy = yx$, alors la profondeur de y est $\leqslant 1$. Plus précisément, il existe b , c , b_1 , $c_1 \in R$ tels que

$$cb_1 = c_1 b , \quad cxb_1 = c_1 xb , \quad \text{et} \quad y = b_1 b^{-1} = c^{-1} c_1 .$$

Ce résultat a encore un caractère assez technique. En voici quelques conséquences:

1° Soit $F = K_k\langle X\rangle$, U son corps de fractions, alors le centre de U est k (pourvu que $\mathrm{card}(X) \geqslant 2$) ; si $x \in X$, alors le centralisateur de x dans U est k(x) .

C'est un résultat assez naturel, mais pas évident a priori. D'ailleurs on aimerait avoir la généralisation suivante :

Si $c \in U$, $c \notin K$, alors le centralisateur de c est de la forme k(t) pour un élément t de V .

C'est un pendant au théorème de Bergman sur les centralisateurs dans $k\langle X\rangle$.

2° Soit F , U comme dans le 1°, et soit $a \in R$ non algébrique sur K . Alors son centralisateur C dans U est algébrique sur k(a) .

Si k est algébriquement clos, on en déduit (en utilisant le théorème de Tsen, cf. [4]) que C est commutatif.

3° Soit k un corps commutatif algébriquement clos, et soit $U = K_k^0 L$ un corps produit de corps sur k . Alors tout automorphisme intérieur de U , qui transforme K en soi-même, est induit par un élément de K .

6. Pour résumer, la méthode qui permet d'étudier les numérateurs et les dénominateurs directement, nous donne des résultats assez fragmentaires, jusqu'à présent, mais j'ai bon espoir que cela pourra devenir un moyen de fournir des informations sur plusieurs questions liées aux corps gauches :

(i) Problème de Lüroth. Est-ce que tout sous-corps de type fini d'un corps libre est encore libre ? Pour un seul générateur, c'est le théorème classique ; l'extension dans le cas commutatif est faux, mais cela ne préjuge pas la question générale.

(ii) Problème de conjugaison dans un corps libre : Donner des conditions pour que deux éléments d'un corps libre soient conjugués.

(iii) Lemme de Britton pour des corps gauches (qui donne une description des relations dans une extension HNN).

Il y a beaucoup de problèmes analogues, pour des "corps libre à involution", des corps ordonnés, des corps valués, etc. En particulier, l'étude des anneaux de valuation dans un corps gauche (cf. [3]) semble rendre plus proche la possibilité de faire de la géométrie algébrique non commutative.

BIBLIOGRAPHIE

[1] COHN (P. M.). - Free rings and their relations. - London, New York, Academic Press, 1971 (London mathematical Society Monographs, 2).

[2] COHN (P. M.). - Full modules over a semifir (à paraître).

[3] MATHIAK (K.). - Bewertungen nicht kommutativer Körper (à paraître).

[4] SERRE (J.-P.). - Corps locaux. - Paris, Hermann, 1962 (Act. scient. et ind., 1296 ; Publ. Inst. Math. Univ. Nancago, 8).

(Texte reçu le 11 juin 1975)

Paul M. COHN
Bedford College
University of London
LONDON NW1 4NS
(Grande-Bretagne)