

Réductibilité des opérateurs aux différences finies : une approche Galois-théorique

Raphaël Bomboy

► **To cite this version:**

Raphaël Bomboy. Réductibilité des opérateurs aux différences finies : une approche Galois-théorique. RR-3735, INRIA. 1999. <inria-00072930>

HAL Id: inria-00072930

<https://hal.inria.fr/inria-00072930>

Submitted on 24 May 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

***Réductibilité des opérateurs aux différences finies :
une approche Galois-théorique***

Raphaël Bomboy

N° 3735

Juillet 1999

————— THÈME 2 —————



***Rapport
de recherche***

Réductibilité des opérateurs aux différences finies : une approche Galois-théorique

Raphaël Bomboy

Thème 2 — Génie logiciel
et calcul symbolique
Projet CAFÉ

Rapport de recherche n° 3735 — Juillet 1999 — 12 pages

Résumé : Nous établissons dans ce document le lien entre les propriétés de réductibilité d'un opérateur aux différences finies linéaire L et la structure de son espace de solution V sous l'action de son groupe de Galois. Dans le cas où L est complètement réductible, nous donnons une description complète de son Eigenring.

Mots-clés : équations aux différences finies, théorie de Galois, réductibilité, Eigenring

Reducibility of linear difference operators : a Galois-theoretic perspective

Abstract: In this document, we state the relation between the reducibility properties of a finite difference operator L and the structure of the associated solution space V under the action of its Galois group. When L is completely reducible, we give a full description of the Eigenring of L .

Key-words: finite difference equations, Galois theory, reducibility, Eigenring

Introduction

Le but de cet article est de donner des critères Galois-théoriques de réductibilité des opérateurs aux différences finies linéaires.

Soit k un corps à différence finie, i.e. un corps muni d'un automorphisme σ . On peut munir l'ensemble des polynômes en la variable σ d'une multiplication en posant, pour tout $a \in k$,

$$\sigma * a = \sigma(a)\sigma$$

et en l'étendant de manière naturelle. Nous noterons $k[\sigma]$ l'anneau ainsi obtenu, et appellerons ses éléments opérateurs aux différences finies linéaires. L'anneau $k[\sigma]$ est non commutatif en général, euclidien à gauche et à droite (voir [1]).

Soit $L = a_n\sigma^n + \dots + a_m\sigma^m$ un opérateur aux différences finies linéaire, avec a_n et a_m non nuls. Nous appellerons $n - m$ l'ordre de L , et nous le noterons $ord(L)$.

Un opérateur aux différences finies L sera dit réductible si et seulement si il existe $L_1, L_2 \in k[\sigma]$, d'ordres strictement inférieurs, tels que $L = L_1 * L_2$.

Soit $L \in k[\sigma]$, $L(y) = 0$ l'équation aux différences finies associée (nous assimilerons souvent L et cette équation), V son espace de solution, G son groupe de Galois (pour les notions de théorie de Galois des équations aux différences finies linéaires, voir [2, 8]). Le but de cet article est de donner des critères de réductibilité de L en fonction de la structure de V en tant que G -module.

Dans la partie 1, nous donnerons des généralités sur le lien entre les propriétés de divisibilité de L et la structure de V .

Dans la partie 2, nous introduirons la notion d'Eigenring d'un opérateur aux différences finies linéaire. L'Eigenring d'un opérateur L est un ensemble d'opérateurs qui nous donne tous les G -endomorphismes de V (proposition 5).

Dans le cas où L est irréductible, son Eigenring est trivial. La réciproque est hélas fautive (voir la fin de la partie 1).

Dans la section 3, nous définirons une classe d'opérateurs (les opérateurs complètement réductibles) dont nous pouvons déterminer complètement la structure de l'Eigenring (proposition 9). Dans ce cas, nous prouverons qu'un opérateur est irréductible si et seulement si son Eigenring est trivial.

L'essentiel de cet article est l'adaptation au cas des équations aux différences finies linéaires de [6], qui traite des mêmes problèmes pour les équations différentielles linéaires.

Dans [7], S.P. Tsarev a prouvé indépendamment qu'un opérateur aux différences finies linéaire complètement réductible était irréductible si et seulement si son Eigenring était non trivial, et donné la structure de l'Eigenring d'un opérateur se décomposant en produit de deux opérateurs irréductibles en employant uniquement des techniques élémentaires.

L'interprétation Galois-théorique des problèmes de réductibilité nous a paru cependant suffisant pour mériter une rédaction séparée.

Rappels et conventions Dans tout l'article, et sauf indication contraire, k désignera un corps à différence finie, σ le morphisme associé, C_k son corps de constantes, L un opérateur aux différences finies linéaire à coefficients dans k .

Dans [2] il est montré qu'un tel opérateur admet une unique (à isomorphisme près) extension de Picard-Vessiot, que nous noterons R . Le groupe de Galois de cette extension sera noté G .

Soit R une extension de Picard-Vessiot de k , associée à un opérateur aux différences finies quelconque, et L un opérateur aux différences finies à coefficients dans k , d'ordre n ; nous appellerons espace des solutions de L dans R , et noterons $Sol_R(L)$, l'ensemble des éléments de R solutions de l'équation associée à L . Notons que $Sol_R(L)$ est un C_k -espace vectoriel. Quand nous parlerons de l'espace des solutions de L (sans précision), il s'agira de l'espace V des solutions de L dans son extension de Picard-Vessiot.

Soit $m \in \mathbb{N}$, $x_1, \dots, x_m \in Sol_R(L)$. Le Casoratien de x_1, \dots, x_m est la matrice

$$C(x_1, \dots, x_m) = \begin{pmatrix} x_1 & \dots & x_m \\ \vdots & & \vdots \\ \sigma^{m-1}(x_1) & \dots & \sigma^{m-1}(x_m) \end{pmatrix}$$

Dans le cas où $m = n$, cette matrice est inversible si et seulement si x_1, \dots, x_n sont C_k -linéairement indépendants. Nous appellerons alors x_1, \dots, x_n un système fondamental de solutions de L , et $Sol_R(L)$ un espace complet de solutions de L . Toute solution de L dans R est alors une C_k -combinaison linéaire de x_1, \dots, x_n (voir [2, Appendix A]).

Soit k un corps à différence finie. Nous noterons S l'anneau des suites à valeurs dans k , muni du morphisme de décalage envoyant la suite $(x_n)_{n \in \mathbb{N}}$ sur la suite $(x_{n+1})_{n+1 \in \mathbb{N}}$, et quotienté par la relation d'équivalence identifiant deux suites égales à partir d'un certain rang. Notons que $k(z)$ s'injecte dans S par l'application envoyant F sur la suite $(F(0), \dots, F(n), \dots)$, complétée arbitrairement aux points où F n'est pas définie.

1 Réductibilité, groupe de Galois et espaces de solutions

Proposition 1 *Soit k un corps à différence finie, L_1 et L_2 deux opérateurs aux différences finies à coefficients dans k . On a équivalence entre les propositions suivantes :*

1. L_1 divise L_2 à droite.
2. Il existe une extension de Picard-Vessiot S de k telle que $Sol_S(L_1) \subseteq Sol_S(L_2)$ et $Sol_S(L_1)$ soit un espace complet de solutions pour L_1 .

3. Pour toute extension de Picard-Vessiot S de k telle que $Sol_S(L_2)$ soit un espace complet de solutions pour L_2 , $Sol_S(L_1) \subseteq Sol_S(L_2)$ et $Sol_S(L_1)$ est un espace complet de solutions de L_1 .

Démonstration $3 \Rightarrow 2$ est trivial.

Montrons que $2 \Rightarrow 1$. L'anneau $k[\sigma]$ étant euclidien à droite, il existe $Q, R \in k[\sigma]$, avec R d'ordre inférieur à L_1 , tel que

$$L_2 = Q.L_1 + R$$

D'après l'égalité ci-dessus, R est nul sur tout l'espace $Sol_S(L_1)$. Or, d'après [2, Appendix A], un opérateur aux différences finies linéaire ne peut avoir dans S un espace vectoriel de solutions de dimension supérieure à son ordre, d'où $R = 0$.

Montrons que $1 \Rightarrow 3$.

On a $L_2 = Q.L_1$, avec $Q \in k[\sigma]$.

Soient n_1 et n_2 les ordres respectifs de L_1 et L_2 , S une extension de Picard-Vessiot de k telle que $\dim(Sol_S(L_2)) = n_2$. L'opérateur L_1 envoie $Sol_S(L_2)$ dans $Sol_S(L_1)$. D'après le théorème du rang

$$\dim(Im(L_1)) + \dim(Ker(L_1)) = n_2$$

Or

$$\dim(Im(L_1)) \leq ord(Q) = n_2 - n_1$$

d'où $\dim(Ker(L_1)) \geq n_1$ et L_1 a n_1 solutions indépendantes dans S .

Corollaire 1 Soit k un corps à différence finie, L_1 et L_2 deux opérateurs aux différences finies à coefficients dans k . On a équivalence entre les propositions suivantes :

1. L_1 et L_2 sont premiers entre eux à droite.
2. Il existe $P_1, P_2 \in k[\sigma]$ tels que $P_1 L_1 + P_2 L_2 = 1$.
3. Soit R_1 (respectivement R_2) une extension de Picard-Vessiot de k telle que $Sol_{R_1}(L_1)$ soit un espace complet de solutions pour L_1 (respectivement $Sol_{R_2}(L_2)$ un espace complet de solutions pour L_2). Alors R_1 ne contient pas de solution non-triviale de L_2 (respectivement L_1).
4. Pour toute extension de Picard-Vessiot R de k , R ne comprend pas de solution non-triviale commune à L_1 et L_2 .

Démonstration L'équivalence entre 1 et 2 n'est rien d'autre que le lemme de Bezout appliqué à l'anneau (euclidien à droite) $k[\sigma]$.

$4 \Rightarrow 3$ est trivial.

Montrons que $2 \Rightarrow 4$. Soit R une extension de k , x un élément de R annulant L_1 et L_2 . On a $(P_1L_1 + P_2L_2)(x) = x = 0$.

Montrons que $3 \Rightarrow 1$.

Supposons que L_1 et L_2 ne soient pas premiers entre eux à droite. Soit L un facteur commun à droite non trivial de L_1 et L_2 . Soit R_1 l'extension de Picard-Vessiot associée à L_1 . D'après la proposition 1, R_1 contient une solution non triviale de L , et cette solution est également une solution de L_2 .

La proposition 1 lie la factorisabilité d'un opérateur aux différences finies L à l'existence d'un sous-espace de son espace de solutions qui soit l'espace de solutions d'une équation de d'ordre plus petit. La proposition suivante lie l'existence de tels espaces à celle d'espaces stables par le groupe de Galois.

Proposition 2 [2, Lemme A.6]

Soit k un corps à différences finies, R une extension de Picard-Vessiot de k , G son groupe de Galois. Soit $V \subset R$ un C_k -espace vectoriel de dimension finie ; V est stable par G si et seulement si V est un espace fondamental de solutions d'une équation aux différences finies à coefficients dans k .

Nous laissons le lecteur se référer à l'article cité pour la démonstration.

Nous pouvons maintenant énoncer notre critère fondamental d'irréductibilité d'une équation.

Proposition 3 [2, Corollaire A.7]

Soit k un corps à différence finie, L une équation aux différences finies linéaire à coefficients dans k , R l'extension de Picard-Vessiot associée à L , V son espace de solutions, G son groupe de Galois. Alors L est irréductible si et seulement si V est G -irréductible.

La démonstration en est évidente d'après la proposition 1 et le corollaire 2.

Corollaire 2 Soit L une équation aux différences finies irréductible à coefficients dans un corps à différences finies k , V son espace de solutions, G son groupe de Galois. Alors $End_G(V) \simeq C_k$.

La démonstration en est immédiate d'après la proposition 3 et le lemme de Schur. (Pour le lemme de Schur, voir par exemple [4, Ch. XVII].)

Remarque La réciproque du corollaire 2 est fautive. Soit en effet l'opérateur aux différences finies à coefficients dans $\mathbb{C}(z)$

$$\sigma^2(x) - 2 \frac{z^2 + 5z + 5}{z + 1} \sigma(x) + 4 \frac{(z + 2)^2}{z + 1} = 0$$

Injectons $C(z)$ dans S tel qu'expliqué dans l'introduction. On vérifie aisément que les suites $(2^n)_{n \in \mathbb{N}}$ et $((n + 1)! \cdot 2^n)_{n \in \mathbb{N}}$ forment une base de solutions de l'équation associée.

Le sous-anneau de S engendré par ces deux suites est l'extension de Picard-Vessiot associée à l'équation (voir [2, Prop. 4.1]) et son groupe de Galois est l'ensemble des matrices du type

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

avec a et b dans \mathbb{C} .

L'ensemble des matrices commutant avec toutes les matrices ci-dessus est réduit aux matrices homotéties, mais l'opérateur n'est pas irréductible car

$$\sigma^2(x) - 2\frac{z^2 + 5z + 5}{z + 1}\sigma(x) + 4\frac{(z + 2)^2}{z + 1} = (\sigma + 2\frac{(z + 2)^2}{z + 1}) * (\sigma - 2)$$

Nous venons de voir que si un opérateur aux différences finies est irréductible, l'ensemble des G -endomorphismes d'un espace de solution associé est isomorphe à C_k , mais que la réciproque est fautive. Dans la partie 3, nous présenterons une classe d'opérateurs, les opérateurs complètement réductibles, pour lesquels cette réciproque est vraie.

Un outil puissant pour l'étude des G -endomorphismes d'un espace de solutions est la notion d'Eigenring, que nous présentons maintenant.

2 Eigenring

Soit (k, σ) un corps à différences finies ; nous noterons \mathcal{E} l'algèbre $k[\sigma]$. Cette algèbre peut être trivialement munie d'une structure de \mathcal{E} -module.

pour tout $L \in k[\sigma]$, nous noterons $\mathcal{E}/\mathcal{E}L$ le \mathcal{E} -module obtenu en quotientant \mathcal{E} par le sous-module des multiples à gauches de L .

Notons que l'existence d'une division euclidienne à droite nous assure que toute classe de $\mathcal{E}/\mathcal{E}L$ admet un unique (à un coefficient multiplicatif près) représentant d'ordre strictement inférieur à celui de L .

Soit L_1, L_2 deux opérateurs aux différences finies à coefficients dans un même corps à différence finie k . Pour tout $L \in \mathcal{E}$, nous noterons \widehat{P} (respectivement \overline{P}) la classe de P dans $\mathcal{E}/\mathcal{E}L_1$ (respectivement $\mathcal{E}/\mathcal{E}L_2$).

Pour tout $L \in \mathcal{E}$, si L_1L est un multiple de L_2 à gauche, il en est de même pour tout élément de la classe de L dans $\mathcal{E}/\mathcal{E}L_2$.

On appellera Eigenring de (L_1, L_2) et on notera $E(L_1, L_2)$ l'ensemble des éléments \overline{L} de $\mathcal{E}/\mathcal{E}L_2$ tels que L_1L est un multiple de L_2 à gauche. (Dans le cas où $L_1 = L_2$, nous simplifierons la notation en $E(L)$.)

Proposition 4 Soient $L_1, L_2 \in \mathcal{E}$. On a bijection entre les ensembles suivants :

- $E(L_1, L_2)$

- $\text{Hom}_{\mathcal{E}}(\mathcal{E}/\mathcal{E}L_1, \mathcal{E}/\mathcal{E}L_2)$

De plus, dans le cas où L_1 et L_2 ont même ordre, cette bijection envoie l'ensemble $E^*(L_1, L_2)$ des éléments \overline{L} de $E(L_1, L_2)$ tels que L et L_2 n'ont pas de facteurs communs à droite sur l'ensemble des isomorphismes de $\mathcal{E}/\mathcal{E}L_1$ vers $\mathcal{E}/\mathcal{E}L_2$.

Démonstration Soit $\overline{L} \in E(L_1, L_2)$. On peut associer à \overline{L} un morphisme

$$\begin{array}{ccc} \phi_L & : & \mathcal{E} \rightarrow \mathcal{E}/\mathcal{E}L_2 \\ & & P \rightarrow PL \end{array}$$

Ce morphisme est indépendant du représentant de la classe \overline{L} choisi.

La classe de L dans $\mathcal{E}/\mathcal{E}L_2$ étant un élément de $E(L_1, L_2)$, il existe $Q \in \mathcal{E}$ tel que $L_1L = QL_2$.

Soit $P \in \mathcal{E}$ un multiple de L_1 à gauche, $R \in L$ tel que $P = RL_1$. On a $\phi_L(P) = \overline{PL} = \overline{RL_1P} = \overline{RQL_2} = \overline{0}$. L'application ϕ_L se factorise donc en un morphisme $\tilde{\phi}_L$ de $\mathcal{E}/\mathcal{E}L_1$ vers $\mathcal{E}/\mathcal{E}L_2$.

Supposons que le morphisme ainsi défini soit nul. On a alors $\tilde{\phi}_L(\widehat{1}) = \overline{1.L} = \overline{L} = \overline{0}$. L'application qui à \overline{L} associe $\tilde{\phi}_L$ est donc injective.

Réciproquement, soit $\tilde{\phi}$ un \mathcal{E} -morphisme de $\mathcal{E}/\mathcal{E}L_1$ vers $\mathcal{E}/\mathcal{E}L_2$, \overline{L} l'image par ce morphisme de $\widehat{1}$.

Pour tout $\widehat{P} \in \mathcal{E}/\mathcal{E}L_1$, $\tilde{\phi}(\widehat{P}) = \tilde{\phi}(P.\widehat{1}) = P.\tilde{\phi}(\widehat{1}) = P.\overline{L} = \overline{PL} = \tilde{\phi}_L(\widehat{P})$. L'application qui à \overline{L} associe $\tilde{\phi}_L$ est donc surjective.

On se place maintenant dans le cas où L_1 et L_2 ont même ordre.

Soit $\overline{L} \in E(L_1, L_2)$ tel que L et L_2 soient premiers entre eux à droite. D'après le théorème de Bezout, il existe $P, Q \in \mathcal{E}$ tels que $PL + QL_2 = 1$.

Pour tout $\overline{R} \in \mathcal{E}/\mathcal{E}L_2$, $\overline{R} = \overline{(R.(PL + QL_2))} = \overline{RPL} = \tilde{\phi}_L(RP)$.

Le morphisme $\tilde{\phi}_L$ est donc surjectif, donc bijectif car $\mathcal{E}/\mathcal{E}L_1$ et $\mathcal{E}/\mathcal{E}L_2$ ont même dimension en tant que k -espaces vectoriels.

Réciproquement, si $\tilde{\phi}_L$ est bijective, $\overline{1}$ à un antécédent pour $\tilde{\phi}_L$, d'où il existe $\widehat{P} \in \mathcal{E}/\mathcal{E}L_1$ tel que $\overline{PL} = \overline{1}$, i.e. $PL + QL_2 = 1$ pour un polynôme $Q \in \mathcal{E}$, d'où L et L_2 sont premiers entre eux à droite.

Proposition 5 Soit L_1 et L_2 deux équations aux différences finies linéaires à coefficients dans un même corps à différence finie k , R une extension de Picard-Vessiot de k contenant deux espaces complets V_1 et V_2 pour L_1 et L_2 , G son groupe de Galois. On a bijection entre les ensembles suivants

- $E(L_1, L_2)$

- $End_G(V_2, V_1)$

Démonstration Soit $\bar{P} \in E(L_1, L_2)$, $P = \sum_{i=0}^n a_i \sigma^i$. On définit le morphisme ϕ_P qui à tout $y \in V_2$ associe $\sum_{i=0}^n a_i \sigma^i(y)$ (ce morphisme ne dépend pas du représentant choisi pour la classe \bar{P}).

Il existe $Q \in \mathcal{E}$ tel que $L_1 P = Q L_2$. Pour tout $y \in V_2$, $L_1 P(y) = Q L_2(y) = 0$, i.e. $\phi_P(y) \in V_1$. De plus, P étant à coefficients dans k , pour tout $g \in G$, $\phi_P(g(y)) = P(g(y)) = g(P(y))$, et ϕ_P est bien un G -endomorphisme de V_2 dans V_1 .

Soit \bar{P} tel que ϕ_P soit le morphisme nul. Pour tout $y \in V_2$, $P(y) = 0$, d'où, d'après la proposition 1, L_2 divise P à droite et la classe de P dans $\mathcal{E}/\mathcal{E}L_2$ est $\bar{0}$. L'application $P \rightarrow \phi_P$ est injective.

Soit enfin $\phi \in End_G(V_2, V_1)$. Soit n_1 et n_2 les ordres respectifs de L_1 et L_2 , x_1, \dots, x_{n_2} un système fondamental de solutions de L_2 . Le Casoratien de $C(x_1, \dots, x_{n_2})$ est inversible et on a donc

$$C(\phi(x_1), \dots, \phi(x_{n_2})) = C(\phi(x_1), \dots, \phi(x_{n_2})).C(x_1, \dots, x_{n_2})^{-1}.C(x_1, \dots, x_{n_2})$$

Soit $A = C(\phi(x_1), \dots, \phi(x_{n_2})).C(x_1, \dots, x_{n_2})^{-1}$. Pour tout $g \in G$, $g(A) = A$, donc A est à coefficients dans k d'après [8, Lemme 1.28]. Notons a_{ij} le coefficient de la $i^{\text{ème}}$ ligne, $j^{\text{ème}}$ colonne de A . Pour tout $y \in V_2$, $\phi(y) = \sum_{j=0}^{n_2-1} a_{1j} \sigma^j(y)$, d'où ϕ est bien le G -morphisme associé au polynôme $\sum_{j=0}^{n_2-1} a_{1j} \sigma^j$.

Remarque Chaque polynôme P nous donne donc une manière canonique -indépendante de l'extension R choisie- de définir un G -morphisme de V_2 dans V_1 .

Dans le cas où L_1 et L_2 sont de même ordre, on peut dire un peu plus encore.

Proposition 6 Soit L_1 et L_2 deux opérateurs aux différences finies de même ordre n , à coefficients dans un même corps à différence finie k . Les propositions suivantes sont équivalentes :

1. $E^*(L_1, L_2)$ est non vide.
2. Il existe une extension de Picard-Vessiot R de k , de groupe de Galois associé G , contenant deux espaces complets de solution G -isomorphe V_1 et V_2 pour L_1 et L_2 .
3. Pour toute extension de Picard-Vessiot R de k , de groupe de Galois associé G , contenant un espace complet de solutions V_2 de L_2 , R contient un espace complet de solution V_1 de L_1 G -isomorphe à V_2

De plus, dans ce cas, l'isomorphisme de la proposition 5 envoie $E^*(L_1, L_2)$ sur l'ensemble des G -isomorphismes de V_2 dans V_1 .

Démonstration 3 \Rightarrow 2 est trivial.

Montrons que 1 \Rightarrow 3. Soit $P \in E(L_1, L_2)$. Pour tout $y \in L_2$, $L_1(\phi_P(y)) = 0$. ϕ_P envoie donc bien V_2 dans l'ensemble V_1 des solutions de L_1 dans R .

Supposons qu'il existe $y \in V_2$ tel que $P(y) = 0$. La proposition 1 nous assure alors que P et L_2 ont un facteur à droite commun, et $P \notin E^*(L_1, L_2)$. Si P est dans $E^*(L_1, L_2)$, il induit donc bien un G -morphisme injectif de V_2 dans V_1 . Dans ce cas, on a nécessairement $\dim(V_1) = n$ et ϕ_P est un isomorphisme de V_2 dans V_1 .

Montrons que 2 \Rightarrow 1. Soit ϕ un G -isomorphisme de V_2 dans V_1 . D'après la proposition 5, il existe $\bar{P} \in E(L_1, L_2)$ tel que $\phi = \phi_{\bar{P}}$.

Soit Q un facteur commun à droite de P et L_2 . D'après la proposition 1, V_2 contient un système fondamental W de solution pour Q . Soit $x \in W$. Q divisant P , on a $\phi_P(x) = P(x) = 0$, d'où comme ϕ est injective $x = 0$. L'espace W est donc réduit à un espace de dimension 0 et Q est constant. D'où L_2 et P n'ont pas de facteur commun à droite non trivial.

3 Opérateurs complètement réductibles

Nous avons vu dans la partie 1 que si un opérateur L était irréductible, son Eigenring était trivial, mais que la réciproque était fausse. Nous définissons maintenant une classe d'opérateurs pour laquelle cette réciproque est vraie.

Définition 1 Soit k un corps à différence finie, L un opérateurs aux différences finies linéaire à coefficients dans k . L est dit complètement réductible si et seulement si il existe L_1, \dots, L_p irréductibles à coefficients dans k tels que $L = \text{ppcmg}(L_1, \dots, L_p)$.

Proposition 7 Soit L un opérateur aux différences finies complètement réductible, L_1, \dots, L_p en nombre minimum tels que $L = \text{ppcmg}(L_1, \dots, L_p)$, V_i l'espace vectoriel des solutions de L_i pour $i \in \{1, \dots, p\}$. Alors, chaque V_i est G -stable, G -irréductible et

$$V = V_1 \oplus \dots \oplus V_p$$

Démonstration Pour tout i , $V_i \subset V$ d'après la proposition 1; V_i est G -stable, et G -irréductible d'après la proposition 3. Les facteurs L_i étant en nombre minimum, ils sont deux à deux premiers entre eux, et les sous-espaces V_i sont en somme directe d'après le corollaire 1.

Soit $W = V_1 \oplus \dots \oplus V_p$. W étant un sous-espace vectoriel de l'extension de Picard-Vessiot associée à L , stable par G , W est l'espace vectoriel de solution d'un opérateur P d'après la proposition 2. Cet espace étant inclus dans V , P divise L à droite d'après la proposition 1.

Pour tout i , $V_i \subset W$ d'où P_i divise P à droite. D'où $L = \text{ppcmg}(L_1, \dots, L_p)$ divise P à droite, et $P = L$ à une constante multiplicative près, d'où $V = W$.

Rappelons quelques définitions et résultats classiques sur les groupes linéaires (voir par exemple [3, 5]). Soit G un tel groupe, V un G -module. V est dit complètement réductible si et seulement si tout sous-espace G -invariant de V admet un complémentaire G -invariant. Ceci équivaut à dire que V se décompose en somme directe de sous-modules G -invariants et G -irréductible.

Un groupe algébrique G est dit réductif si et seulement si son radical unipotent est trivial. Dans le cas où le corps considéré est de caractéristique nulle, cela équivaut à dire que G admet un G -module réductif fidèle. Tout G -module est alors complètement réductible.

Proposition 8 *Soit L une équation aux différences finies linéaire à coefficients dans un corps k , R l'extension de Picard-Vessiot associée, G son groupe de Galois, V l'espace des solutions de L . On a équivalence entre :*

1. L est complètement réductible.
2. V est un G -module complètement réductible.
3. G est un groupe réductif.

Démonstration L'équivalence entre 2 et 3 découle des résultats rappelés avant la proposition.

D'après la proposition 7, $1 \Rightarrow 2$. Réciproquement, supposons que V se décompose sous la forme $V_1 \oplus \dots \oplus V_p$ avec V_i un module G -stable et G -irréductible pour tout i .

D'après la proposition 2, pour tout i , V_i est un espace complet de solutions pour un opérateur aux différences finies L_i . Pour tout i , $V_i \subset V$, L_i divise L à droite d'après la proposition 1, d'où le plus petit commun multiple à gauche M des V_i divise L à droite.

Réciproquement, comme $V = V_1 \oplus \dots \oplus V_p$, toute solution de L est solution de M , d'où L divise M à droite et $L = M$ à une constante multiplicative près.

Proposition 9 *Soit $L = \text{ppcm}g(L_1, \dots, L_p)$ un opérateur aux différences finies complètement réductible d'ordre n à coefficients dans un corps à différence finie k . Il existe des entiers n_1, \dots, n_q , avec $n_1 + \dots + n_q = n$ tels que $E(L) = M_{n_1}(C_k) \oplus \dots \oplus M_{n_q}(C_k)$, où $M_{n_i}(C_k)$ désigne l'ensemble des matrices carrées de taille n_i à coefficients dans C_k . De plus, dans ce cas, L est irréductible si et seulement si $E(L) \simeq C_k$.*

Démonstration Soit V l'espace des solutions de L . Rappelons que d'après la proposition 5, $E(L)$ est isomorphe à l'ensemble des G -isomorphismes de V .

D'après la proposition 7, V peut s'écrire sous la forme $V_1^{n_1} \oplus \dots \oplus V_r^{n_r}$, où les V_i sont des sous-modules G -irréductibles deux à deux non- G -isomorphes. Une conséquence classique du lemme de Schur est alors que

$$\text{End}_G(V) \simeq \bigoplus_{i=1 \dots r} M_{n_i}(\text{End}(V_i))$$

Chaque V_i étant G -irréductible, on a $End(V_i) \simeq C_k$ pour tout i d'après le corollaire 2, d'où

$$End_G(V) \simeq \bigoplus_{i=1 \dots r} M_{n_i}(C_k)$$

De plus, on a $r = n_1 = 1$ si et seulement si V est G -irréductible, i.e. ssi L est irréductible.

Références

- [1] Manuel Bronstein and Marko Petkovsek. An introduction to pseudo-linear algebra. *Theoretical Computer Science*, 157:3–33, 1996.
- [2] P.A. Hendriks and M.F. Singer. Solving difference equations in finite terms. *J. Symbolic Computation*, 27:239–259, 1999.
- [3] James E. Humphreys. *Introduction to Lie Algebras and Representation Theory*. Number 9 in Graduate Texts in Mathematics. Springer-Verlag, 1972.
- [4] Serge Lang. *Algebra*. Addison-Wesley Publishing Company, 3 edition, 1993.
- [5] A.L. Onishchik and E.B. Vinberg. *Lie Groups and Algebraic Groups*. Springer-Verlag, 1990.
- [6] Michael F. Singer. Testing reducibility of linear differential operator : A group theoretic perspective. *Applicable Algebra in Engineering, Communication and Computing*, 7:77–104, 1996.
- [7] S.P. Tsarev. On the factorization algorithm of M. Singer for skew polynomials. *Programirovanie*, Submitted.
- [8] Marius van der Put and Michael F. Singer. *Galois Theory of Difference Equations*. Number 1666 in Lecture Notes in Mathematics. Springer, 1997.



Unité de recherche INRIA Sophia Antipolis
2004, route des Lucioles - B.P. 93 - 06902 Sophia Antipolis Cedex (France)

Unité de recherche INRIA Lorraine : Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - B.P. 101 - 54602 Villers lès Nancy Cedex (France)

Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)

Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38330 Montbonnot St Martin (France)

Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, B.P. 105 - 78153 Le Chesnay Cedex (France)
<http://www.inria.fr>
ISSN 0249-6399