Recurrences over division rings

Ahmed Cherchem (USTHB, Algiers)

Joint work with Abdelkader Necer and Tarek Garici

Lens, July 2013

Preliminaries

R : ring with an identity element which is not necessarily commutative,
M : left $R-$module,
$S(M)$: the set of M-valued sequences $(u : \mathbb{N} \to M)$,
$R[X]$: the algebra of the polynomials with coefficients in the ring R (the indeterminate X commutes with the coefficients of R).

Definition

A sequence $u \in S(M)$ is called a linear recurring sequence if it satisfies a relation of the form

$$\forall n \in \mathbb{N}, u(n+h) = a_{h-1}u(n+h-1) + \cdots + a_1 u(n+1) + a_0 u(n),$$

where $h \in \mathbb{N}$ and $a_i \in R$.

The set of M-valued linear recurring sequences with coefficients in R is denoted $LRS_R(M)$.

Preliminaries

Problem

$$u, v \in LRS_R(M) \Rightarrow u + v \in LRS_R(M)?$$

$$\alpha \in R, u \in LRS_R(M) \Rightarrow \alpha u \in LRS_R(M)?$$

Reference :
Linear recurring sequences over noncommutative rings, *Journal of Algebra and its Applications*,Vol. 11, N°2. (2012)

Preliminaries

The set $S(M)$, endowed with the ordinary addition and multiplication by a scalar is an R-module. We get an $R[X]$-module structure for $S(M)$ by defining, for $p(X) = a_0 + a_1 X + \cdots + a_h X^h \in R[X]$:

$$\begin{aligned} \forall u &\in S(M), \forall n \in \mathbb{N}, \\ (p(X).u)(n) &= a_0 u(n) + a_1 u(n+1) + \cdots + a_h u(n+h). \end{aligned}$$

Let $u \in S(M)$. Denote by I_u the annihilator of u in $R[X]$. We thus have :

$$I_u = \{p \in R[X], \quad p.u = 0\}.$$

$$u \in LRS_R(M) \Leftrightarrow I_u \text{ contains a monic polynomial.}$$

Definitions

A monic polynomial contained in I_u is called characteristic polynomial of u. A characteristic polynomial with minimal degree h is called minimal polynomial of u and h is called order of the sequence u.

If $fu = 0$ and $gv = 0$ with $fg = gf$,then

$$fg\,(u+v) = g\,(fu) + f(gv) = 0.$$

Or, if there exists φ, ψ such that $\varphi f = \psi g$, then

$$\varphi f\,(u+v) = \varphi\,(fu) + \psi(gv) = 0.$$

A counterexample

Example

Let k be an arbitrary ring and $R = k\langle x, y\rangle$ the ring with noncommutative independant indeterminates x and y. Denote by u and v the linear recurring sequences defined over R by :

$$\forall n \in \mathbb{N}, \quad u(n) = x^n \quad \text{and} \quad v(n) = y^n.$$

As $Rx \cap Ry = \{0\}$, then the sequence $u + v$ is not a linear recurring sequence.

Case of division rings

Proposition

Let D be a division ring and M a D-module. Then the set $LRS_D(M)$ of all M-valued linear recurring sequences with coefficients in D is a submodule of the $D[X]$-module $S(M)$.

Remark

If $f(X) = X^h + a_{h-1}X^{h-1} + \cdots + a_0$ is a characteristic polynomial for the linear recurring sequence u, then for all $\alpha \in D$, $\alpha \neq 0$, the polynomial

$$g(X) = X^h + \alpha a_{h-1}\alpha^{-1}X^{h-1} + \cdots + \alpha a_0\alpha^{-1}$$

is a characteristic polynomial for the sequence αu.

Case of finite dimension

Lemma (Jacobson)

Let m and d be two positive integers and let D be a division ring of dimension d over its center F. Then, for any polynomial $f(X) \in D[X]$ of degree m, there exists a nonzero polynomial $g(X) \in D[X]$ of degree $m(d-1)$ such that $f(X)g(X) = g(X)f(X) \in F[X]$.

Case of finite dimension

Determining the polynomial $g(X)$.

$$f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0,$$

$$V = De_1 \oplus De_2 \oplus \cdots \oplus De_m,$$

φ the endomorphisme of V defined by $\varphi(e_i) = e_{i+1}$ if $1 \leq i \leq m-1$, and $\varphi(e_m) = -a_0 e_1 - a_1 e_2 - \cdots - a_{m-1} e_m$.

φ is also an endomorphism of V regarded as a vector space over F. Let h be the characteristic polynomial of φ, then dividing h by f on the right, we obtain g.

Case of finite dimension

Proposition

Let D be a division ring of dimension d over its center F. Let M be a D-module. Let u and v be two elements of $LRS_D(M)$ with minimal polynomials f_1 and f_2 respectively. Set $s = \deg f_1$ and $t = \deg f_2$ and assume $s \leq t$. Let g_1 be the polynomial given by Jacobson's Lemma and corresponding to the polynomial f_1. Then :

1. *The polynomial $f_1 g_1 f_2$ is a characteristic polynomial of the sequence $u + v$,*
2. *The linear recurring sequence $u + v$ has order less than or equal to $ds + t$.*

Example

Let $\mathbb{H}$ be a ring of quaternions with center F and let u and v the sequences defined over $\mathbb{H}$ by the relations :

$$u(0) = 1, u(1) = 0, \text{ and } \forall n \in \mathbb{N}, u(n+2) = iu(n+1) + u(n)$$

$$v(0) = v(1) = v(2) = 1, \text{ and } \forall n \in \mathbb{N}, v(n+3) = v(n+2) + jv(n),$$

with respective characteristic polynomials

$$f_1(X) = X^2 - iX - 1 \text{ and } f_2(X) = X^3 - X^2 - j.$$

Example (cont)

Example

We have $V = \mathbb{H}e_1 \oplus \mathbb{H}e_2$ and the endomorphism φ is given by :

$$\varphi(e_1) = e_2 \text{ and } \varphi(e_2) = e_1 + ie_2.$$

Let $(u_1, \cdots, u_8)$ be the canonical basis of the vector space F^8, and remark that

$$\forall a + bi + cj + dk \in \mathbb{H}, i(a + bi + cj + dk) = -b + ai - dj + ck.$$

Then we have :

$$\begin{aligned} \varphi(u_i) &= u_{i+4} \text{ for } 1 \leq i \leq 4, \\ \varphi(u_5) &= u_1 + u_6, \varphi(u_6) = u_2 - u_5, \\ \varphi(u_7) &= u_3 + u_8, \varphi(u_8) = u_4 - u_7. \end{aligned}$$

Example (cont)

Example

We obtain the matrix :

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix},$$

Example (cont)

Example

with characteristic polynomial

$$h(X) = X^8 - 2X^6 + 3X^4 - 2X^2 + 1.$$

Dividing $h(X)$ by $f_1(X)$, we get

$$g_1(X) = X^6 + iX^5 - 2X^4 - iX^3 + 2X^2 + iX - 1.$$

Therefore $f_1 g_1 f_2$ is a characteristic polynomial for the sequence $u + v$.

Generating function

Definition

Let R be a ring. The generating function of the sequence $u \in S(R)$ is the formal series

$$G_u(X) = \sum_{n \geq 0} u(n) X^n \in R[[X]].$$

Proposition

Let D be a division ring and let $u \in S(D)$. Then the following statements are equivalent :

1. $u \in SRL_D(D)$,
2. *The generating function of u is rational of the form $g^{-1}(X) f(X)$, where $f(X)$ and $g(X)$ are polynomials in $D[X]$ with $g(0) \neq 0$.*

Generating function

Proof.

Let $u \in SRL_D(D)$, with characteristic polynomial $p(X) = X^h - a_1 X^{h-1} - \cdots - a_h \in D[X]$. Set $g(X) = 1 - a_1 X - \cdots - a_h X^h$. The coefficient of X^m in $g(X) G_u(X)$ is equal to 0 for $m \geq h$ and then we have

$$\begin{aligned} & g(X) G_u(X) \\ = \; & u(0) + (u(1) - a_1 u(0)) X + \cdots \\ & + (u(h-1) - a_1 u(h-2) - \cdots - a_{h-1} u(0)) X^{h-1} \\ = \; & f(X). \end{aligned}$$

Hence $G_u(X) = g^{-1}(X) f(X)$, with $g(0) \neq 0$. □

Proof.

Conversely, let $u \in S(D)$ and assume that the generating function of u is (left) rational : $G_u(X) = g^{-1}(X) f(X)$, where $f(X) = a_0 + a_1 X + \cdots + a_h X^h, g(X) = b_0 + b_1 X + \cdots + b_k X^k$ and $b_0 \neq 0$. Then

$$\begin{aligned} & \left(b_0 + b_1 X + \cdots + b_k X^k\right)\left(u(0) + u(1) X + u(2) X^2 + \cdots\right) \\ = \; & b_0 u(0) + (b_0 u(1) + b_1 u(0)) X + \cdots \\ & + \left(b_0 u(h) + \cdots + b_k u(h-k) X^h\right). \end{aligned}$$

Therefore, we obtain for any $n \in \mathbb{N}$,

$$\begin{aligned} & u(n+h+1) \\ = \; & -b_0^{-1}\left(b_1 u(n+h) + b_2 u(n+h-1) + \cdots + b_k u(n+h-k)\right), \end{aligned}$$

hence $u \in SRL_D(D)$. □

THANK YOU