

November 9 – 19, 2021.

Limbe (Cameroun)

Number Theory
I : Linear Recurrent Sequences
African Institute for Mathematical Sciences (AIMS)
Michel Waldschmidt, Sorbonne Université

Assignment 1

Let $d \geq 1$ be an integer and c_1, \dots, c_d complex numbers with $c_d \neq 0$. Define

$$P(T) = T^d - c_1 T^{d-1} - \dots - c_{d-1} T - c_d \in \mathbb{C}[T].$$

Denote by $\gamma_1, \dots, \gamma_\ell$ the distinct roots of P in \mathbb{C} , and, for $1 \leq j \leq \ell$, by t_j the multiplicity of the root γ_j , so that

$$P(T) = \prod_{j=1}^{\ell} (T - \gamma_j)^{t_j}$$

with $t_j \geq 1$, $t_1 + \dots + t_\ell = d$.

Denote by E the vector space over \mathbb{C} of the sequences which satisfy the linear recurrence relation of order d given by

$$u_{n+d} = c_1 u_{n+d-1} + \dots + c_d u_n \quad \text{for } n \geq 0. \quad (1)$$

- (1). Prove that E is a complex vector subspace of $\mathbb{C}^{\mathbb{N}}$ of dimension d .
(2). The goal of this exercise is to prove that a basis of E is given by the d sequences

$$(n^i \gamma_j^n)_{n \in \mathbb{N}} \quad (1 \leq j \leq \ell, \quad 0 \leq i \leq t_j - 1). \quad (2)$$

- (a) Prove this result in the special case $t_1 = \dots = t_\ell = 1$.
(b) Prove this result in the special case $\ell = 1$.

Hint.

Check, for $n \geq 0$ and $0 \leq i \leq d - 1$,

$$\sum_{k=0}^d (-1)^k \binom{d}{k} (d+n-k)^i = 0.$$

- (c) From (a) and (b), deduce this result in the special case $d = 2$.
 Consider now the general case.
 (d) Prove that the d sequences (2) satisfy (1).
 (e) Prove that the d sequences (2) give a basis of E .

Hint. There are several ways of proving (b), (d) and (e). You may use some of the following suggestions.

- (i) For $i \geq 0$, check that the map

$$\begin{array}{ccc} \mathbb{C}[T] & \longrightarrow & \mathbb{C}[T] \\ (T \frac{d}{dT})^i : \sum_{h \geq 0} a_h T^h & \longmapsto & \sum_{h \geq 0} a_h h^i T^h \end{array}$$

is a linear map. We agree that $h^i = 1$ for $i = h = 0$. Check, for $n \geq 0$, $1 \leq j \leq \ell$ and $0 \leq i \leq t_j - 1$,

$$\left(T \frac{d}{dT} \right)^i (T^n P)(\gamma_j) = 0.$$

Deduce

$$(n+d)^i \gamma_j^{n+d} = \sum_{k=1}^d (n+d-k)^i c_k \gamma_j^{n+d-k} \quad (n \geq 0),$$

with the convention that for $k = n+d$, the term $(n+d-k)^i$ takes the value 1 for $i = 0$ and the value 0 for $i \geq 1$. Deduce that for $1 \leq j \leq \ell$ and $0 \leq i \leq t_j - 1$, the sequence $(n^i \gamma_j^n)_{n \geq 0}$ satisfies (1).

- (ii) Write the linear recurrence relation in a matrix form

$$U_{n+1} = CU_n$$

with

$$U_n = \begin{pmatrix} u_n \\ u_{n+1} \\ \vdots \\ u_{n+d-1} \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ c_d & c_{d-1} & c_{d-2} & \cdots & c_1 \end{pmatrix}.$$

Write the matrix C in its Jordan normal form.

(iii) Introduce the formal power series

$$U(T) = \sum_{n \geq 0} u_n T^n.$$

Check that $U(T)$ is a rational fraction, with denominator

$$1 - \sum_{i=1}^d c_i T^i = T^d P(1/T) = \prod_{j=1}^{\ell} (1 - \gamma_j T)^{t_j},$$

while the numerator is of degree $< d$. Use a partial fraction decomposition. Develop $(1 - \gamma_j T)^{-i-1}$ for $0 \leq i \leq t_j - 1$ as a power series expansion. Deduce that the d sequences (2) generate E .

(iv) Consider the matrix A made of ℓ vertical blocks $A_1, A_2, \dots, A_{\ell}$ where for $1 \leq j \leq \ell$, A_j is the $t_j \times d$ matrix

$$A_j = \begin{pmatrix} 1 & \gamma_j & \gamma_j^2 & \cdots & \gamma_j^{t_j-1} & \gamma_j^{t_j} & \cdots & \gamma_j^{d-1} \\ 0 & 1 & \binom{2}{1} \gamma_j & \cdots & \binom{t_j-1}{1} \gamma_j^{t_j-2} & \binom{t_j}{1} \gamma_j^{t_j-1} & \cdots & \binom{d-1}{1} \gamma_j^{d-2} \\ 0 & 0 & 1 & \cdots & \binom{t_j-1}{2} \gamma_j^{t_j-3} & \binom{t_j}{2} \gamma_j^{t_j-2} & \cdots & \binom{d-1}{2} \gamma_j^{d-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \binom{t_j}{t_j-1} \gamma_j & \cdots & \binom{d-1}{t_j-1} \gamma_j^{d-t_j} \end{pmatrix}.$$

Note that $\binom{r}{k} = 0$ for $r < k$.

Show that the d columns of A are linearly independent over \mathbb{C} .

Number Theory
I : Linear Recurrent Sequences
African Institute for Mathematical Sciences (AIMS)

Michel Waldschmidt, Sorbonne Université

Assignment 1 — Solution

(1). We have seen in the course that E is a vector subspace of $\mathbb{C}^{\mathbb{N}}$ of dimension d . Let us repeat the proofs. The sum of two elements in E is in E , the product of an element in E with a constant is in E , hence E is a vector subspace of $\mathbb{C}^{\mathbb{N}}$. We now check that a basis of E is given by the d so-called *impulse* sequences $e^{(0)}, \dots, e^{(d-1)}$ defined by the initial conditions

$$e_n^{(j)} = \delta_{jn} \quad (0 \leq j, n \leq d-1),$$

δ_{jn} being the Kronecker symbol

$$\delta_{jn} = \begin{cases} 1 & \text{if } j = n, \\ 0 & \text{if } j \neq n. \end{cases}$$

We first check that $\{e^{(0)}, \dots, e^{(d-1)}\}$ is a generating set for E . Let $(u_n)_{n \geq 0}$ be in E . By the definition of $e^{(0)}, \dots, e^{(d-1)}$, for $0 \leq n \leq d-1$ we have

$$u_n = u_0 e_n^{(0)} + u_1 e_n^{(1)} + \dots + u_{d-1} e_n^{(d-1)}.$$

Since both u and $u_0 e^{(0)} + u_1 e^{(1)} + \dots + u_{d-1} e^{(d-1)}$ are in E , it follows that there relations are true for all $n \geq 0$. In other words we have

$$u = u_0 e^{(0)} + u_1 e^{(1)} + \dots + u_{d-1} e^{(d-1)}.$$

Hence $\{e^{(0)}, \dots, e^{(d-1)}\}$ is a generating set for E .

Since the matrix $(e_i^{(n)})_{0 \leq i, n \leq d-1}$ is the identity matrix, the d sequences $e^{(0)}, \dots, e^{(d-1)}$ are linearly independent.

(2) The answers have also been given during the course. Here they are.

(a) When $t_1 = \dots = t_\ell = 1$ we have $\ell = d$ and $\gamma_1, \dots, \gamma_d$ are d distinct roots of P . In this case the d sequences $(\gamma_j^n)_{n \geq 0}$ satisfy (1) :

$$\gamma_j^{n+d} = c_1 \gamma_j^{n+d-1} + \dots + c_d \gamma_j^n \quad \text{for } n \geq 0 \text{ and } 1 \leq j \leq d$$

and are linearly independent since the determinant

$$\begin{pmatrix} 1 & \gamma_1 & \gamma_1^2 & \dots & \gamma_1^{d-1} \\ 1 & \gamma_2 & \gamma_2^2 & \dots & \gamma_2^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \gamma_d & \gamma_d^2 & \dots & \gamma_d^{d-1} \end{pmatrix}$$

is not zero (Vandermonde).

(b) When $\ell = 1$ we have $t_1 = d$, $P(T) = (T - \gamma_1)^d$. We want to prove that the d sequences

$$(n^i \gamma_1^n)_{n \geq 0} \quad 0 \leq i \leq d-1 \tag{3}$$

give a basis for E . We first check that they belong to E . Since

$$(T - \gamma_1)^d = T^d - dT^{d-1}\gamma_1 + \binom{d}{2}T^{d-2}\gamma_1^2 - \dots + (-1)^k \binom{d}{k}T^{d-k}\gamma_1^k + \dots + (-1)^d \gamma_1^d,$$

the linear recurrence relations of which this polynomial is the characteristic polynomial is

$$u_{n+d} = du_{n+d-1}\gamma_1 - \binom{d}{2}u_{n+d-2}\gamma_1^2 + \dots + (-1)^{k-1} \binom{d}{k}u_{n+d-k}\gamma_1^k + \dots + (-1)^{d+1}u_n\gamma_1^n.$$

Hence the relation that we need to prove is

$$(n+d)^i = d(n+d-1)^i - \binom{d}{2}(n+d-2)^i + \dots + (-1)^{k-1} \binom{d}{k}(n+d-k)^i + \dots + (-1)^{d+1}n^i \tag{4}$$

for $0 \leq i \leq d-1$ and $n \geq 0$. Here is a proof.

For $n \geq 0$ the polynomial $T^n(T-1)^d$ has a zero at $T=1$ of multiplicity d , hence for $1 \leq i \leq d-1$ and $n \geq 0$ the polynomial

$$\left(T \frac{d}{dT}\right)^i (T^n(T-1)^d)$$

vanishes at $T = 1$. From

$$T^n(T-1)^d = T^{n+d} - dT^{n+d-1} + \binom{d}{2}T^{n+d-2} - \dots + (-1)^k \binom{d}{k}T^{n+d-k} + \dots + (-1)^d T^n$$

and

$$\left(T \frac{d}{dT}\right)^i (T^h) = h^i T^h$$

we deduce

$$\begin{aligned} \left(T \frac{d}{dT}\right)^i (T^n(T-1)^d) &= (n+d)^i T^{n+d} - d(n+d-1)^i T^{n+d-1} \\ &+ \binom{d}{2} (n+d-2)^i T^{n+d-2} - \dots + (-1)^k \binom{d}{k} (n+d-k)^i T^{n+d-k} + \dots + (-1)^d n^i T^n. \end{aligned}$$

Substituting $T = 1$ gives (4).

That these d sequences (3) give a basis for E amounts to saying that the matrix

$$\begin{pmatrix} 1 & \gamma_1 & \gamma_1^2 & \gamma_1^3 & \cdots & \gamma_1^n & \cdots & \gamma_1^{d-1} \\ 0 & \gamma_1 & 2\gamma_1^2 & 3\gamma_1^3 & \cdots & n\gamma_1^n & \cdots & (d-1)\gamma_1^{d-1} \\ 0 & \gamma_1 & 4\gamma_1^2 & 9\gamma_1^3 & \cdots & n^2\gamma_1^n & \cdots & (d-1)^2\gamma_1^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \vdots \\ 0 & \gamma_1 & 2^{d-1}\gamma_1^2 & 3^{d-1}\gamma_1^3 & \cdots & n^{d-1}\gamma_1^n & \cdots & (d-1)^{d-1}\gamma_1^{d-1} \end{pmatrix}$$

is regular. Since γ_1 is not zero, this is equivalent to saying that the determinant of the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & \cdots & 1 \\ 0 & 1 & 2 & 3 & \cdots & n & \cdots & (d-1) \\ 0 & 1 & 4 & 9 & \cdots & n^2 & \cdots & (d-1)^2 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \vdots \\ 0 & 1 & 2^{d-1} & 3^{d-1} & \cdots & n^{d-1} & \cdots & (d-1)^{d-1} \end{pmatrix}$$

is nonzero. Since the polynomial

$$\frac{X(X-1)\cdots(X-n+1)}{n!}$$

has degree n , by linear combinations of the rows we see that this determinant is the product by $1!2! \cdots (d-1)!$ with the determinant of the upper triangular matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & \cdots & 1 \\ 0 & 1 & \binom{2}{1} & \binom{3}{1} & \cdots & \binom{n}{1} & \cdots & \binom{d-1}{1} \\ 0 & 0 & 1 & \binom{3}{2} & \cdots & \binom{n}{2} & \cdots & \binom{d-1}{2} \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \binom{n}{k} & \cdots & \binom{d-1}{k} \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

hence it is not zero.

(c) When $d = 2$, the polynomial P has degree 2, and either

- P has two distinct roots γ_1 and γ_2 , which means $\ell = d = 2$, $t_1 = t_2 = 1$. In this case we are in the situation of (a), the two sequences $(\gamma_1^n)_{n \geq 0}$ and $(\gamma_2^n)_{n \geq 0}$ give a basis of E ,

or

- P has a double root γ , which means $\ell = 1$, $t_1 = 2$, and in this case we are in the situation of (b). The sequence $(n\gamma_1^n)_{n \geq 0}$ satisfies (1) and the two sequences $(\gamma_1^n)_{n \geq 0}$ and $(n\gamma_1^n)_{n \geq 0}$ give a basis of E .

In fact Quiz 1 gives a direct answer to (c).

(e) We use the method suggested by (i) to prove that the d sequences (2) are in E .

Since γ_j is a root of multiplicity t_j of $T^n P(T)$, γ_j is a root of the polynomials

$$\left(\frac{d}{dT} \right)^i (T^n P(T))$$

for $0 \leq i \leq t_j - 1$. For $0 \leq i \leq t_j - 1$, the polynomial $(T \frac{d}{dT})^i (T^n P(T))$ is a linear combinations of the polynomials $(\frac{d}{dT})^k (T^n P(T))$ with $0 \leq k \leq i$. Hence for $1 \leq j \leq \ell$ and $0 \leq i \leq t_j - 1$ the number γ_j is a root of the polynomials

$$\left(T \frac{d}{dT} \right)^i (T^n P(T)).$$

From

$$T^n P(T) = T^{n+d} - c_1 T^{n+d-1} - \cdots - c_d T^n$$

we deduce

$$\left(T \frac{d}{dT}\right)^i (T^n P(T)) = (n+d)^i T^{n+d} - c_1(n+d-1)^i T^{n+d-1} - \dots - c_d n^i T^n.$$

Since γ_j is a root of this polynomial, we get, for $n \geq 0$, $1 \leq j \leq \ell$ and $0 \leq i \leq t_j$,

$$(n+d)^i \gamma_j^{n+d} = c_1(n+d-1)^i \gamma_j^{n+d-1} - \dots - c_d n^i \gamma_j^n.$$

This means that the sequences $(n^i \gamma_j^n)_{n \geq 0}$ for $1 \leq j \leq \ell$, $0 \leq i \leq t_j$ satisfy (1).

(e) We use the method suggested by (ii) to prove that the d sequences (2) generate E .

Let $(u_n)_{n \geq 0}$ be an element in E . Write the linear recurrence relation in a matrix form

$$U_{n+1} = CU_n$$

with

$$U_n = \begin{pmatrix} u_n \\ u_{n+1} \\ \vdots \\ u_{n+d-1} \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ c_d & c_{d-1} & c_{d-2} & \cdots & c_1 \end{pmatrix}.$$

Write the matrix C in its Jordan normal form :

$$P^{-1}CP = J \quad \text{where} \quad J = \begin{pmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_\ell \end{pmatrix}$$

and

$$J_j = \begin{pmatrix} \gamma_j & 1 & 0 & \cdots & 0 & 0 \\ 0 & \gamma_j & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & \gamma_j & 1 \\ 0 & 0 & 0 & \cdots & 0 & \gamma_j \end{pmatrix} \quad (1 \leq j \leq \ell)$$

For $n \geq 0$ we have

$$J^n = \begin{pmatrix} J_1^n & 0 & \cdots & 0 \\ 0 & J_2^n & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_\ell^n \end{pmatrix}$$

and, for $1 \leq j \leq \ell$,

$$J_j^n = \begin{pmatrix} \gamma_j^n & \binom{n}{1}\gamma_j^{n-1} & \binom{n}{2}\gamma_j^{n-2} & \cdots & \binom{n}{t_j-2}\gamma_j^{n-t_j+2} & \binom{n}{t_j-1}\gamma_j^{n-t_j+1} \\ 0 & \gamma_j^n & \binom{n}{1}\gamma_j^{n-1} & \cdots & \binom{n}{t_j-3}\gamma_j^{n-t_j+3} & \binom{n}{t_j-2}\gamma_j^{n-t_j+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \binom{n}{1}\gamma_j^{n-1} & \binom{n}{2}\gamma_j^{n-2} \\ 0 & 0 & 0 & \cdots & \gamma_j^n & \binom{n}{1}\gamma_j^{n-1} \\ 0 & 0 & 0 & \cdots & 0 & \gamma_j^n \end{pmatrix}.$$

From the matrix relation $U_n = C^n U_0$ we deduce

$$U_n = P^{-1} J^n P U_0.$$

Hence there exist complex numbers c_{ij} such that, for all $n \geq 0$,

$$u_n = \sum_{j=1}^{\ell} \sum_{i=0}^{t_j-1} c_{ij} n^i \gamma_j^n.$$

This proves that any element of E is a linear combination of the sequences (2), hence that these d sequences are a system of generators of E . Since E has dimension d , it shows that these sequences (2) are a basis of E .

(e) We use the method suggested by (iii) to prove again that the d sequences (2) generate E .

The left hand side of the product $\left(1 - \sum_{i=1}^d c_i T^i\right) U(T)$ is a telescoping series

$$\left(1 - \sum_{i=1}^d c_i T^i\right) U(T) = \sum_{j=0}^{d-1} \left(u_j - \sum_{i=1}^j c_i u_{j-i}\right) T^j.$$

Hence $U(T)$ is a rational fraction, with denominator

$$1 - \sum_{i=1}^d c_i T^i = T^d P(1/T) = \prod_{j=1}^{\ell} (1 - \gamma_j T)^{t_j},$$

while the numerator is of degree $< d$. Using a partial fraction decomposition, we write this rational fraction as

$$U(T) = \sum_{j=1}^{\ell} \sum_{i=0}^{t_j-1} \frac{q_{ij}}{(1 - \gamma_j T)^{i+1}}.$$

For $1 \leq j \leq \ell$, we develop $(1 - \gamma_j T)^{-i-1}$ as a power series expansion :

$$\frac{1}{(1 - \gamma_j T)^{i+1}} = \frac{1}{i! \gamma_j^i} \left(\frac{d}{dT} \right)^i \frac{1}{1 - \gamma_j T} = \sum_{n \geq 0} \frac{(n+1)(n+2) \cdots (n+i)}{i!} \gamma_j^n T^n.$$

It follows that u_n is a linear combination of the elements γ_j^n with coefficients being polynomials of degree $< t_j$ evaluated at n .

(e) We use the method suggested by (iii) to prove again that the d sequences (2) are linearly independent.

This amounts to showing that the determinant of the matrix A is different from 0. Let us define s_j to be

$$s_j = t_1 + \cdots + t_{j-1} \quad \text{for } 1 \leq j \leq \ell \text{ with } s_1 = 0.$$

For $1 \leq j \leq \ell$, $0 \leq i \leq t_j - 1$, $0 \leq k \leq d - 1$, the $(s_j + i, k)$ entry of the matrix A is

$$\frac{1}{i!} \left(\frac{d}{dT} \right)^i T^k \Big|_{T=\gamma_j} = \binom{k}{i} \gamma_j^{k-i}.$$

Let C_0, \dots, C_{d-1} denote the d columns of A and let b_0, \dots, b_{d-1} be complex numbers such that

$$b_0 C_0 + \cdots + b_{d-1} C_{d-1} = 0.$$

The left side of this equality is an element of \mathbb{C}^d , the d components of which are all 0, and these d relations mean that the polynomial

$$b_0 + b_1 T + \cdots + b_{d-1} T^{d-1}$$

vanishes at the point γ_j with multiplicity at least t_j for $1 \leq j \leq \ell$. Since $t_1 + \cdots + t_\ell = d$, we deduce that $b_0 = \cdots = b_{d-1} = 0$.

Références

- [1] Everest, Graham ; van der Poorten, Alf ; Shparlinski, Igor ; Ward, Thomas. *Recurrence sequences*, Mathematical Surveys and Monographs (AMS, 2003), volume **104** (1290 references). Zbl MR
- [2] Andrica, Dorin ; Bagdasar, Ovidiu. Recurrent sequences. Key results, applications, and problems. Problem Books in Mathematics, Springer 2020. Zbl MR
- [3] Levesque, Claude and Waldschmidt, Michel. Linear recurrence sequences and twisted binary forms. Proceedings of the International Conference on Pure and Applied Mathematics ICPAM-GOROKA 2014, South Pacific Journal of Pure and Applied Mathematics, vol. 2, No 3 (2015), 65-83. arXiv:1802.05154 [math.NT].

Further references are available from my website

<http://www.imj-prg.fr/~michel.waldschmidt/>

See in particular

<http://www.imj-prg.fr/~michel.waldschmidt/AgendaArchives.html>

January 25 - 28, 2021. Limbe (Cameroun) - online

A course on *linear recurrent sequences* at the African Institute for Mathematical Sciences (AIMS) Cameroun.

1. *The square root of 2, the Golden ratio and the Fibonacci sequence*. Link to the video.
 2. *Linear recurrence sequences*. Part I, examples. Link to the video.
 3. *Linear recurrence sequences*. Part II, the theory.. Link to the video.
 4. *On the Brahmagupta-Fermat-Pell Equation* Link to the video.
- Quizz 1. Quizz 2. Tutorial 1*, January 26, 2021. *Tutorial 2*, January 28, 2021. *Assignment. Tutorial 3*.