

Formal power series and applications - Tutorial 02

Yahia Idriss Benalioua

University of Warsaw

2026/10/13

Exercise 1 (Minimal polynomials).

1. Show that an algebraic formal power series is not always uniquely determined by its minimal polynomial.
2. Suppose the minimal polynomial $P \in \mathbb{Q}(x)[y]$ of an algebraic series f has more than one formal power series root. Can there be another polynomial $Q \in \mathbb{Q}(x)[y]$ that uniquely characterizes f ?
3. Give examples of polynomials that admit exactly one formal power series root, and examples of polynomials that admit none.

Solution.

1. Let $f = \sqrt{1-4x} = 1 - \sum_{n=1}^{\infty} \frac{2}{n} \binom{2n-2}{n-1} x^n$ (see Exercise 4). It is an algebraic series verifying $f^2 - 1 - 4x = 0$, but its minimal polynomial $P = y^2 - 1 - 4x$ also admits $-f \neq f$ as a root.
2. That's impossible because, by minimality of P , any polynomial $Q \in \mathbb{Q}(x)[y]$ vanishing on f must be a multiple of P . Consequently, any formal power series root of P must also be a root of Q .
3. Any polynomial verifying the conditions of the implicit power series theorem must have a unique power series root. Take e.g. $P = y^2 - xy - y$, we have $P(0,0) = 0$ and $\frac{\partial P}{\partial y} = 2y - x - 1$, thus $\frac{\partial P}{\partial y}(0,0) = -1 \neq 0$ and P has a unique power series root.

Let $P = y^2 - x$. If P admitted a power series root f , then $f^2 = x$, meaning that $1 = \text{ord}(x) = \text{ord}(f^2) = 2\text{ord}(f)$, which is impossible.

□

Exercise 2 (Composition of formal power series). Let $f, g \in \mathbb{Q}[[x]]$.

1. Under which conditions does the composition $f \circ g$ exist?
2. Show that rational and algebraic series are closed under composition.

Solution.

1. We can show that $f \circ g$ exists if and only if $g(0) = 0$.

If $g(0) \neq 0$, then the constant term for $f \circ g$ would be an infinite sum, which is not always defined in general.

Conversely, if $g(0) = 0$, then $\text{ord}(g^n) \geq n$ for all $n \in \mathbb{N}$ and all the coefficients of $f \circ g$ are defined by finite sums.

See [1, Section 2.3] or [2, Section 1.1] for more formal details.

2. Let $f = \frac{P}{Q}$ and $g = \frac{R}{S}$ with $P, Q, R, S \in \mathbb{Q}[x]$ be two rational series. We have $f \circ g = \frac{P(R/S)}{Q(R/S)}$, which is well-defined since $Q(R/S)(0) = Q(g(0)) = Q(0) \neq 0$ as a direct consequence of the conditions for the definition of f and $f \circ g$. Moreover, it is clearly rational since it can be rewritten as the quotient of two polynomials.

For algebraic series, we can use the characterization that a power series f is algebraic if and only if there exists a finite dimensional algebra A such that $f \in A$, to show the result as follows.

Let $f, g \in \mathbb{Q}[[x]]$ such that $f^d = \sum_{i=0}^{d-1} p_i(x) f^i$ and $g^r = \sum_{i=0}^{r-1} q_i(x) g^i$ for some $p_0, \dots, p_{d-1}, q_0, \dots, q_{r-1} \in \mathbb{Q}(x)$. Let

$$A = \text{Lin}_{\mathbb{Q}(x)}(\{(f^i \circ g)g^j \mid 0 \leq i \leq d-1 \text{ and } 0 \leq j \leq r-1\})$$

Obviously, $f \circ g \in A$, and it remains to show that A is closed by products. Clearly, it is enough to show that $f^d \circ g \in A$ and $g^r \in A$. For g^r , by definition $g^r \in \text{Lin}_{\mathbb{Q}(x)}(g^0, \dots, g^{r-1}) \subseteq A$. As for $f^d \circ g$, we have

$$f^d \circ g = \left(\sum_{i=0}^{d-1} p_i(x) f^i \right) \circ g = \sum_{i=0}^{d-1} p_i(g) f^i \circ g$$

which is an element of A since the $p_i(g) \in \text{Lin}_{\mathbb{Q}(x)}(g^0, \dots, g^{r-1})$. □

Exercise 3 (Compositional inverses). *Let $f \in \mathbb{Q}[[x]]$ be a power series. It admits a right compositional inverse if there exists $g \in \mathbb{Q}[[x]]$ such that $f(g(x)) = x$.*

1. *When does f admit a right compositional inverse?*
2. *If f admits a right compositional inverse, does it admit a left compositional inverse?*
3. *If f admits a right compositional inverse and is algebraic, is the inverse also algebraic?*

Solution. Let us first make some useful observations. Let $f = \sum_{n \in \mathbb{N}} f_n x^n$ and let $g = \sum_{n \in \mathbb{N}} g_n x^n$ with $g(0) = g_0 = 0$. For all $n \in \mathbb{N}$, $\text{ord}(g) \geq n$. Thus $[x^n]f \circ g = [x^n](\sum_{k=0}^n f_k g^k) = \sum_{k=0}^n f_k [x^n]g^k$. Moreover, $[x^n]g^k = \sum_{i_1 + \dots + i_k = n} g_{i_1} \dots g_{i_k}$. Thus,

$$[x^n]f \circ g = \sum_{k=0}^n f_k \sum_{i_1 + \dots + i_k = n} g_{i_1} \dots g_{i_k} \quad (1)$$

1. f admits a right compositional inverse if and only if $f(0) = 0$ and $\frac{df}{dx}(0) \neq 0$.

Indeed, if there exists $g \in \mathbb{Q}[[x]]$ such that $f \circ g = x$, then $f \circ g(0) = f(0) = 0$ and, by (1), $[x]f \circ g = f_1 g_1 = \frac{df}{dx}(0) \frac{dg}{dx}(0) = 1$ and thus $\frac{df}{dx}(0) \neq 0$.

Conversely, if $f(0) = 0$ and $\frac{df}{dx}(0) \neq 0$, then we can define g such that $f \circ g = x$ inductively as follows. For the composition to be well defined we must have $g(0) = 0$. Moreover, by identifying the coefficients of $f \circ g$ and x , we have $g_1 = \frac{1}{f_1}$, and $[x^n]f \circ g = 0$ for all $n \geq 2$. Thus, by (1), $g_n = \frac{-1}{f_1} \sum_{k=2}^n f_k \sum_{i_1+\dots+i_k=n} g_{i_1} \dots g_{i_k}$ is defined as a function of the values of the previous g_i .

2. If f admits a right compositional inverse g , then, by the previous question, g verifies the same conditions and admits a right compositional inverse h . But, by associativity, $h = (f \circ g) \circ h = f \circ (g \circ h) = f$, and g is also the left compositional inverse of f .

Thus, the formal power series verifying the conditions described in the previous question form a group whose operation is composition. The compositional inverse of f is usually denoted by $f^{(-1)}$.

3. If f is algebraic then there exists $P \in \mathbb{Q}[x, y]$ such that $P(x, f) = 0$. If $f^{(-1)}$ is the compositional inverse of f , then $0 = P(x, f) = P(f^{(-1)}, f^{(-1)} \circ f) = P(f^{(-1)}, x)$ and $f^{(-1)}$ is thus algebraic.

□

Exercise 4 (Algebraic series and context-free languages). *Determine the number of words of length $2n$ in the Dyck language, i.e. the language of well-parenthesized words.*

Hint: you may use the identity $\sqrt{1-4x} = 1 - \sum_{n=1}^{\infty} \frac{2}{n} \binom{2n-2}{n-1} x^n$ to avoid tedious calculations (this can be shown using the generalized binomial theorem).

Solution. Let $f = \sum_{n \in \mathbb{N}} f_n x^n$ where f_n is the number of words of length $2n$ in the Dyck language. Consider the unambiguous context-free grammar defined by its rules $S \rightarrow \epsilon | (S)S$ generating the Dyck language.

By translating the rules of the grammar, we obtain $f = 1 + x f^2$. Note that, since we're counting pairs of parentheses, the second rule yields $x f^2$ instead of $x^2 f^2$.

Solving the quadratic equation, we obtain either $f = \frac{1+\sqrt{1-4x}}{2x}$ or $f = \frac{1-\sqrt{1-4x}}{2x}$. The positive root is excluded since $f(0) = 1$. Thus

$$\begin{aligned} f &= \frac{1 - \sqrt{1-4x}}{2x} \\ &= \frac{1}{2x} \sum_{n=1}^{\infty} \frac{2}{n} \binom{2n-2}{n-1} x^n \\ &= \sum_{n=1}^{\infty} \frac{1}{n} \binom{2n-2}{n-1} x^{n-1} \\ f &= \sum_{n \in \mathbb{N}} \frac{1}{n+1} \binom{2n}{n} x^n \end{aligned}$$

Finally, $f_n = \frac{1}{n+1} \binom{2n}{n}$, which is the n -th Catalan number.

See [3, Chapter 6] for a (very long) list of combinatorial structures counted by the Catalan numbers. $\square$

Exercise 5 (Showing transcendence).

1. Show that e^x is not an algebraic power series.
2. We will now show Eisenstein's theorem, which can be stated as follows: if $f = \sum_{n \in \mathbb{N}} f_n x^n \in \mathbb{Q}[[x]]$ is algebraic, then there exists a positive integer M such that $M^n f_n \in \mathbb{Z}$ for all $n \in \mathbb{N}$.
 - (a) Show that for all $f \in \mathbb{Q}[[x]]$ with $f(0) = 0$, if there exists $Q \in \mathbb{Z}[x]$ such that, $Q(x, f) = 0$, $Q(0, 0) = 0$ and $\frac{\partial Q}{\partial y}(0, 0) = c \neq 0$ then $f(c^2 x) \in \mathbb{Z}[[x]]$.
 - (b) Prove Eisenstein's theorem.
3. Deduce an alternative proof of the transcendence of e^x .
4. Is the converse of Eisenstein's theorem true?

Solution.

1. By contradiction, suppose that e^x is algebraic, then there exists a minimal $d \in \mathbb{N}$ such that

$$\sum_{i=0}^d p_i(x) e^i x = 0 \quad (2)$$

for some $p_0, \dots, p_d \in \mathbb{Q}(x)$. Without loss of generality, we can assume that $p_d = 1$. By derivation, we obtain

$$\sum_{i=0}^d p'_i(x) e^i x + i p_i(x) e^i x = 0 \quad (3)$$

Subtracting d times the equation (2) from (3) we obtain

$$\sum_{i=0}^{d-1} (p'_i(x) + (i-d)p_i(x)) e^i x = 0$$

contradicting the minimality of d .

The rest of the questions will be answered in the next tutorial. $\square$

References

- [1] Manuel Kauers and Peter Paule. *The Concrete Tetrahedron: Symbolic Sums, Recurrence Equations, Generating Functions, Asymptotic Estimates*. Texts and Monographs in Symbolic Computation. Springer-Verlag Wien, 1 edition, 2011.

- [2] Richard P. Stanley. *Enumerative Combinatorics, Volume 1*, volume 1 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2nd edition edition, 2011.
- [3] Richard P. Stanley. *Enumerative Combinatorics, Volume 2*, volume 2 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2nd edition edition, 2023.