Artin-Hasse Exponential

and an Introduction to p-adics

Achyut Bharadwaj, Swayam Chaulagain, Krittika Garg, Lex Harie Pisco
Counsellor: Sanskar
Mentor: Nischay

PROMYS India

Jun 16, 2023

1. Power Series

2. Introduction to p-adics

3. Analysis in $\mathbb{Q}_p$

Table of Contents

Ring of Formal Power Series

We define a formal power series of a ring R to be the set $R[[x]] = \{\sum_{n \geqslant 0} a_n x^n \, | a_n \in R\}$. We define an addition and multiplication operation on $R[[x]]$ as follows:

- Let $f(x) = \sum_{n \geqslant 0} a_n x^n$ and $g(x) = \sum_{n \geqslant 0} b_n x^n$. Then, we define

$$f(x) + g(x) = \sum_{n \geqslant 0} (a_n + b_n) x^n$$

  where $a_n + b_n$ is carried out in R.

- Let $f(x) = \sum_{n \geqslant 0} a_n x^n$ and $g(x) = \sum_{n \geqslant 0} b_n x^n$. Then, we define

$$f(x) \cdot g(x) = \sum_{k \geqslant 0} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k$$

  where $a_i \cdot b_{k-i}$ is carried out in R.

It turns out that R is a ring under the operations defined above.

Units of $R[[x]]$

Proposition

An element $f(x) \in R[[x]]$ is a unit in R if and only if $f(0)$ (the first term of the power series) is a unit in R.

Proof.

If $f(0)$ is not a unit, then: Let us assume that there is some g such that $fg = 1$ where $f(x) = \sum_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum_{i=0}^{\infty} b_i x^i$. Thus,

$$f(x)g(x) = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k = 1$$

Hence, $a_0 b_0 = 1$ and $\sum_{i=0}^{k} a_i b_{k-i} = 0$ for all $k \geqslant 1$. So, $b_0 = a_0^{-1}$. But, if a_0 is not a unit, its inverse does not exist. Contradiction. Thus, a_0 must be a unit.

Now, suppose that a_0 is a unit. Then, we have $b_0 = 1/a_0$. Now, when $k = 1$, we have $a_0 b_1 + b_0 a_1 = 0$. Thus, $b_1 = -\frac{b_0 a_1}{a_0}$ which clearly exists. By induction, we can keep going on and find each such b_i and hence the corresponding $g(x)$ required. Thus, an inverse power series exists. □

Composition of Power Series

Proposition

For $f(x), g(x) \in R[[x]]$, we have $f(g(x)) \in R[[x]]$ if and only if $g(0) = 0$.

Example

Consider $f(x) = 1 + x + x^2 + \cdots$ in $\mathbb{Z}[[x]]$.

- Consider $g(x) = 1$. Then, clearly $f(g(x)) = f(1) = 1 + 1 + \cdots$ which does not make sense. Hence, $f(g(x))$ is not defined in this case.
- Consider $g(x) = x^2$. Then, we have $f(g(x)) = 1 + x^2 + x^4 + \cdots$ which is clearly an element of $R[[x]]$ too.

Multivariate Power Series

We now extend formal power series to multiplie variables.

- We define $R[[x,y]]$ to be $(R[[x]])[[y]]$
- More generally, we define $R[[x_1,\ldots,x_n]]$ to be $(R[[x_1,\ldots,x_{n-1}]])[[x_n]]$ inductively.
- By induction, one can see that if R is a ring, then $R[[x_1,\ldots,x_n]]$ is also a ring.

Polynomial Fields and Rational Functions

For some field k, we write $k[x]$ to denote the set of polynomials with coefficients in k.

$$k(x) := \left\{ \frac{g(x)}{h(x)} \mid g, h \in k[x], h(x) \neq 0 \right\}$$

Firstly, we explore the relation between $k(x), k[x]$ and $k[[x]]$.

- $k[x] \subset k(x)$ (set $h(x) = 1$)
- $k[x] \subset k[[x]]$
- If $h(0) \neq 0$, then $g(x)/h(x)$ can be expressed as a unique power series $t(x) \in k[[x]]$. This is called the power series expansion of $g(x)/h(x)$.

The Coefficients of a Power Series Expansion

Proposition

If $t(x)$ is the power series expansion of a rational function, then the coefficients, a_n of $t(x)$ satisfy a linear recursion. That is, there exists some number $m \geqslant 1$ and and constants $c_1, \ldots, c_m \in k$ such that for all sufficiently large n, we have

$$a_n = \sum_{i=1}^{m} c_i a_{n-i}$$

Example

$g(x) = 2x + 1$ and $h(x) = x^2 + 1$. Then,

$$\frac{g(x)}{h(x)} = \frac{2x+1}{x^2+1} = 1 + x + 2x - x^3 - 2x^4 + x^5 + 2x^6 - \cdots$$

Notice how the terms of the power series are recursive.

Proof

Proof.

Suppose we have $t(x) = g(x)/h(x)$ where $t(x)$ is a power series and g, h are polynomials in $k[x]$. Therefore, we have $g(x) = t(x)h(x)$. Now, $g(x)$ has finite degree and so does $h(x)$. However, $t(x)$ is a power series and need not have a finite degree. Let the degrees of $h(x), g(x)$ be m, k respectively. Next, we evaluate the expansion of the product $t(x)h(x)$ and combine the terms of like degree. Now, for some n that is greater than both m and k, we must have that the coefficient of x^n is 0. Thus we get

$$a_n b_0 + \cdots a_{n-m} b_m = 0$$

for all n that is greater than both m and k. This gives us a linear recurrence relation for a_n:

$$a_n = -\frac{a_{n-1}b_1 + \cdots + a_{n-m}b_m}{b_0}$$

□

Coefficients

Now, the converse of the previous proposition also holds. That is, if the coefficients of $t(x)$ satisfy a linear recurrence relation, then $t(x)$ is the power series expansion of some rational function. This can be proven by simply reversing the arguments of the converse.

Table of Contents

A Leftist Introduction

In our usual system we write numbers in the normal decimal system from left to right. Let us explore a new number system. Let us instead write the numbers from right to left. This is called as the leftist number system. Here are some rules to follow:

- Normally, we write a real number such as π as $3.141592\ldots$. In the leftist number system, rather than writing the three dots to the right, we write the three dots to the left. For example, leftist 1 can be expressed as $...0001$.
- The process of leftist addition and multiplication are similar to that in the rightist system.

Example

Add $\ldots 9997$ to $\ldots 0003$. Multiply $...6667$ with $..003$. Multiply $...00624$ with $...0625$.

Some Leftist Properties

- **Negative numbers** in the rightist system can be represented as a leftist number without adding a negative sign. For example, rightist -3 is leftist $...9997$.
- **Rational numbers** in the rightist system can be represented as a leftist number without adding a division sign. For example, $1/3 = ...6667$.
- Leftist numbers in normal decimal system(base 10) have **zero divisors**. In other words, we can find two non-zero leftist numbers in base 10 that multiply to give 0. An example is $...90625$ and $...90624$.
- Normally, the decimal expansion of a real number such as 1234 is

$$1 \times 10^3 + 2 \times 10^2 + 3 \times 10 + 4$$

similarly, we can expand the leftist number $...1234$ as:

$$\cdots + 1 \times 10^3 + 2 \times 10^2 + 3 \times 10 + 4$$

where the expansion continues indefinitely to the left.

Leftists in Other Bases

Now, instead of using base-10, we can use some other base, say p where p is a prime. In base 3, $...0112$ is a leftist number which can be represented as

$$\cdots + 2 \times 3^2 + 1 \times 3 + 2$$

Now, consider the set of all leftist numbers in base p. That is, the set of all numbers of the form

$$x_0 + x_1 p + x_2 p^2 + \cdots$$

The p-adic Integers

We can rewrite this series as a sequence of partial sums as follows:

$$x_0 + x_1 p + x_2 p^2 + \cdots \rightarrow (x_0, x_0 + x_1 p, x_0 + x_1 p + x_2 p^2, \ldots)$$

Now, let $a_1 = x_0, a_2 = x_0 + x_1 p, \ldots$. We call this set $\mathbb{Z}_p = (a_1, a_2, ...)$, the p-adic integers. Notice that:

- For all i, we have $a_i \in \mathbb{Z}/p^i\mathbb{Z}$ since $x_i \in \mathbb{Z}/p\mathbb{Z}$, where $\mathbb{Z}/p\mathbb{Z}$ is the ring of integers modulo p.
- For every k, we have $a_{k+1} \equiv a_k \pmod{p^k}$ since all terms up to p^k are the same.

We will see later why this sequencial definition of $\mathbb{Z}_p$ is needed to make things simpler, rather than just calling $\mathbb{Z}_p$ as the set of all leftist numbers.

The Ring of $\mathbb{Z}_p$

Recall that the set of leftist numbers had an addition operation. We define an equivalent addition operation on our alternative definition of $\mathbb{Z}_p$ as done in the previous slide. Take $a = (a_1, a_2, \dots)$ and $b = (b_1, b_2, \dots)$. We define addition and multiplication as follows:

- $a + b = (a_1 + b_1, a_2 + b_2, \dots)$
- $ab = (a_1 b_1, a_2 b_2, \dots)$

Example

Convince yourself that the operations defined above are equivalent to the operations defined on the set of leftist numbers of base p.

Properties of $\mathbb{Z}_p$

- $\mathbb{Z}_p$ forms a ring and has no zero divisors. Moreover, $\mathbb{Z} \subset \mathbb{Z}_p$.
- An element a of $\mathbb{Z}_p$ is a unit if and only if $a_1 \not\equiv 0 \pmod{p}$.
- We say $a \equiv b \pmod{p^k}$ if $a_i = b_i$ for all $1 \leqslant i \leqslant k$.
- Every element of $\mathbb{Z}_p$ can be expressed as $a = p^k u$ where k is a nonnegative integer and u is a unit.

Hensel's lifting Lemma

Proposition

Let $f(x)$ be a polynomial with coefficients in $\mathbb{Z}_p$. Let $a_1 \in \mathbb{Z}/p\mathbb{Z}$ so that $f(a_1) \equiv 0 \pmod{p}$ and $f'(a_1) \not\equiv 0 \pmod{p}$. Then, there exists a unique $a \in \mathbb{Z}_p$ such that $a \equiv a_1 \pmod{p}$ and $f(a) = 0$.

Example

Let $f(x) = x^3 - 3$. Then, $f(2) = 5 \equiv 0 \pmod{5}$ say $= 5k$ and $f'(2) \equiv 3(2)^2 \equiv 2 \neq 0 \pmod{5}$. So we can apply hensel lemma that implies the existence of $a_2 = 5m + 2$ such that $f(a_2) \equiv 0 \pmod{25}$. The proof of hensel's lemma gives us the unique value of $m = -k(f'(a_1))^{-1}$. In this case k would be 1 and $(f'(a_1))^{-1} = 3$. So $a_2 = 12$. Indeed by inspection we can see $f(12) \equiv 0 \pmod{25}$

Expansion of leftist number in reals

Example

Evaluate the leftist number $...222$ of base 3 in the reals.

Sol.

We have $...222 + ...001 = ...000$ by performing addition. Thus, $.the..222 = -1$.

Now, we may also write $...222 = 2 + 2 \times 3 + 2 \times 3^2 + 2 \times 3^3 + \cdots$. If we use the formula for an infinite geometric progression, we get

$$...222 = \frac{2}{1-3} = -1$$

which gives the correct answer. However, the geometric series formula is only valid when $|r| < 1$. Yet, we arrived at the correct answer by substituting $r = 3$.

Leftist Convergence

Notice that series that do not normally converge, such as $2 + 2 \times 3 + \cdots$, converge in the leftist numbers. Therefore, it is safe to conclude that the "$+$" operation that is being performed is not being performed in $\mathbb{R}$. We must therefore come up with some other system of numbers in which series such as the one above converge.

Constructing the p-adic Numbers

In order to deal with the problem explained in the previous slide, we now construct a new number system, called the p-adics, which we will denote by $\mathbb{Q}_p$. Now, notice that any rational number can be expressed as a leftist number. Therefore, $\mathbb{Q}$ is contained in $\mathbb{Q}_p$. This gives us an idea: Can we construct $\mathbb{Q}_p$ from $\mathbb{Q}$? Can we do it in the same way that we construct $\mathbb{R}$ from $\mathbb{Q}$? How do we do so? Following is how $\mathbb{R}$ is constructed from $\mathbb{Q}$.

- A Cauchy sequence is a sequence of rational numbers (x_n) so that the absolute value of the difference between the terms approaches 0. In other words, as $m, n \to \infty$ we have $|x_n - x_m| \to 0$. In other words, a Cauchy sequence is a sequence of rational numbers which we want to converge in our to be defined system, $\mathbb{R}$.
- Now take the set of Cauchy sequences, S. For each element of S, find the limit of each sequence.
- The set of these limits is $\mathbb{R}$.

p-adic Absolute Value

We can similarly construct $\mathbb{Q}_p$ from $\mathbb{Q}$ as well. But there is a major difference. Consider the previous example of the leftist number $2 + 2 \times 3 + \cdots$ in base 3. This converges to -1 when evaluated in base 3. However, it is very obvious to see that under the normal absolute value, this sequence, i.e. $(2, 2 + 2 \times 3, \dots)$ is not a Cauchy sequence. Thus, in order to define $\mathbb{Q}_p$ in the way we defined $\mathbb{R}$ from $\mathbb{Q}$, we need to define a new notion of the absolute value.

Definition

We define $v_p(a)$ where a is an integer to be the highest power of p that divides a. We define $v_p(q)$ where q is a rational number of the form a/b to be $v_p(a) - v_p(b)$.

Definition

We define the p-adic absolute value of a rational number q to be $|q|_p = p^{-v_p(q)}$.

What does $|\cdot|_p$ Measure?

Notice that the newly defined p-adic absolute value measures inversely, the size of the power of k in the rational number. That is to say, if the power of p is high, then the number is p-adically small and if the power is small, the number is p-adically small. To make sense of this, we can think of the p-adic absolute value as something that measures up to what degree two rational numbers are equal. If we take the two rationals modulo p^k for each k, the two rational numbers are closer if they start to differ at a higher power k.

The Ultrametric

The p-adic absolute value satisfies the following properties:

- $|q|_p \geqslant 0$. Equality occurs if and only if $q = 0$
- $|qr|_p = |q|_p |r|_p$
- $|q + r|_p \leqslant |q|_p + |r|_p$

Notice how all these properties are satisfied by the absolute value in the reals too. Functions that satisfy the above are known as metrics (of a given space, which is $\mathbb{Q}$ in this case). However, there is one major difference between the p-adic metric and the absolute value:

$$|q + r|_p \leqslant \max\left(|q|_p, |r|_p\right)$$

A metric satisfying the above is called an ultrametric. This property leads to huge differences between the reals and the p-adics. An example which we will see later is that this leads to a much simpler condition for convergence in $\mathbb{Q}_p$ than in $\mathbb{R}$, where we have multiple different convergence tests.

The p-adic Numbers

We define the p-adic numbers, similar to the reals as follows:

- A p-adic Cauchy sequence is a sequence such that the p-adic absolute value of higher terms get closer to each other.
- Now take the set of p-acid Cauchy sequences, S_p. For each element of S_p, find the limit of each sequence.
- The set of these limits is $\mathbb{Q}_p$.

The p-adic Integers Revisited

We define the p-adic integers $\mathbb{Z}_p$ to be

$$\mathbb{Z}_p := \{a \in \mathbb{Q}_p \mid |a|_p \leqslant 1\}$$

Example

Prove that the above definition of $\mathbb{Z}_p$ is equivalent to the previous definition of $\mathbb{Z}_p$ as a sequence (Hint: Use the leftist numbers).

Table of Contents

Sequences in $\mathbb{Q}_p$

- We can extend the p-adic absolute value to elements of $\mathbb{Q}_p$ itself. Let (a_i) be a sequence so that $a = \lim_{n\to\infty} a_n \in \mathbb{Q}_p$. Then, we define the p-adic absolute value of a to be the limit of the p-adic absolute value of a_n as n goes to infinity. This turns out to be well defined.
- From this, we can show that a sequence (a_n) where $a_n \in \mathbb{Q}_p$ converges in $\mathbb{Q}_p$ if and only if the sequence $(|a_n|_p)$ converges in $\mathbb{R}$. Moreover, the absolute value of the limit of (a_n) equals the limit of the absolute value of a_n. That is, $|\lim_{n\to\infty} a_n|_p = \lim_{n\to\infty} |a_n|_p$.
- Another property is that the series $\sum_{n\geqslant 0} a_n$ converges if and only if the sequence (a_n) converges to 0.

Power Series in $\mathbb{Q}_p$

Recall that we can have a power series over any ring R. Since $\mathbb{Q}_p$ is a ring, we can have one over $\mathbb{Q}_p$ too. Call it $\mathbb{Q}_p[[x]]$.

- We say that the power series $f(x) = \sum_{n\geqslant 0} a_n x^n$ converges at $t \in \mathbb{Q}_p$ if the series $\sum_{n\geqslant 0} a_n t^n$ converges in $\mathbb{Q}_p$.
- The series converges if and only if $|a_n t^n|_p$ converges to 0 in $\mathbb{R}$.
- We define the radius of convergence of a power series in $\mathbb{Q}_p$ to be the positive real r so that for all $c < r$ we have $|a_n|_p c^n$ converges to 0 and for all $c > r$ the same sequence diverges. This can be thought of as the largest p-adic absolute value for which all p-adic absolute value less than r, the series diverges.
- The radius of convergence is given by $r = \left(\limsup {a_n}^{1/n}\right)^{-1}$

From Power Series to Functions

We define discs as follows:

- **Open disc:** The open disc of radius r centered at a is defined to be $D\left(a;r^{-}\right) := \{z \in \mathbb{Q}_p \mid |z-a|_p < r\}$
- **Closed disc:** The closed disc of radius r centered at a is defined to be $D\left(a;r\right) := \{z \in \mathbb{Q}_p \mid |z-a|_p \leqslant r\}$

We have also shown that the open disc is a closed set, likewise for the closed disc is an open set. (Hint: Pick a boundary point in the open disc, and observe the relation with the non-archimedean inequality, and see if you can still apply the same argument for the closed disc). Now, we can define a function

$$f : D\left(0;r^{-}\right) \to \mathbb{Q}_p$$

which evaluates to

$$\lim_{n\to\infty}\left(\sum_{n\geqslant 0} a_n x^n\right)$$

for any x in the respective domain.

Continuity of $f(x)$

The function, $f\colon D(0;r^-) \to \mathbb{Q}_p$ is continuous. In other words, for every $y \in \mathbb{Q}_p$ and $s \in \mathbb{R}_{>0}$ such that the preimage of $D(y;s^-)$ under f is a union of open discs. Which is given by,

$$f^{-1}(D(y;s^-)) = \{a \in D(0;r^-) | f(a) \in D(y;s^-)\}$$

For a sketch-proof, fix an element of the preimage of $D(y;s^-)$ under f, and see the relation with convergence in $\mathbb{Q}_p$. Hence we have,

$$f^{-1}(D(y;s^-)) = \bigcup_{|t|_p<r} D(t;r^-)$$

Exponentiation in $\mathbb{Q}_p$

We want to define an exponential function in $\mathbb{Q}_p$ similar to e^x in $\mathbb{R}$. In order to do so, recall the power series of e^x in $\mathbb{R}$. We have

$$e^x = \sum_{n \geqslant 0} \frac{x^n}{n!}$$

We similarly define $\exp(x)$ in $\mathbb{Q}_p$ as the following power series

$$\exp(x) = \sum_{n \geqslant 0} \frac{x^n}{n!}$$

The $\exp(x)$ function in $\mathbb{Q}_p$ behaves differently from that in $\mathbb{R}$ in several ways. As an example, the radius of convergence of $\exp(x)$ in $\mathbb{Q}_p$ is not infinity. We have proven that the radius of convergence of $\exp(x)$ is $p^{-1/(p-1)}$ in $\mathbb{Q}_p[[x]]$. (Hint: Observe the relation of $v_p(n!)$ with the digits of n over base p)

Properties of $\exp$

Some properties of $\exp$ remain the same in $\mathbb{Q}_p$, while some other differ:

- The domain of $\exp(x)$ is $D\left(0; \left(p^{-1/(p-1)}\right)^{-}\right)$. Note how this differs from the domain of $\exp$ in $\mathbb{R}$ which is the whole of $\mathbb{R}$.
- $\exp(a+b) = \exp(a) \cdot \exp(b)$
- $\exp(a)^n = \exp(na)$
- $\forall x, y \in D\left(0; \left(p^{-1/(p-1)}\right)^{-}\right), \left|\exp(x) - \exp(y)\right|_p = |x-y|_p$. Observe how this is neater than in $\mathbb{R}$. This property does not hold in $\mathbb{R}$.

Logarithms in $\mathbb{Q}_p$

We define the logarithm power series as follows:

$$\log(1+x) = \sum_{n\geqslant 1} (-1)^{n+1} \frac{x^n}{n}$$

replicating the power series expansion of $\log$ in the reals. The radius of convergence of this series turns out to be 1. Moreover, when $|1+x|_p = 1$, the series converges as well. Thus, the domain will be $D\left(1; 1^-\right)$. This can also be expressed as $1 + p\mathbb{Z}_p$.

Properties of the Logarithm

- The domain of $\log(x)$ is $1 + p\mathbb{Z}_p$
- $\log(ab) = \log(a) + \log(b)$
- $\log(a^n) = n \log(a)$

Logarithm as an Inverse of Exponentiation

- We see that when $s \in D\left(0; \left(p^{-1/(p-1)}\right)^-\right)$ we have

$$\exp(s) \in D\left(1; \left(p^{-1/(p-1)}\right)^-\right)$$

  which is a subset of $D(1; 1^-)$. Hence, the composition of $\log$ and $\exp$ exists.
- Moreover, $\log(\exp(s)) = s$ for all $s \in D\left(0; \left(p^{-1/(p-1)}\right)^-\right)$.
- When $s \in D\left(1; \left(p^{-1/(p-1)}\right)^-\right)$ we have $\log(s) \in D\left(0; \left(p^{-1/(p-1)}\right)^-\right)$. Hence the composition of $\exp$ and $\log$ exists.
- Moreover, $\exp(\log(s)) = s$ for all $s \in D\left(0; \left(p^{-1/(p-1)}\right)^-\right)$.

This shows that $\log$ and $\exp$ are inverse functions of each other. However, note that they are inverses only when s is in a specific local range, unlike in $\mathbb{R}$, where they are inverses of each other for all of $\mathbb{R}$.

Artin-Hasse Exponential Function

The Artin-Hasse Exponential is defined as follows:

$$E(x) = \exp\left(\sum_{n \geqslant 0} \frac{x^{p^n}}{p^n}\right)$$

While the above exponential seems random, it turns out that this exponential has some interesting properties. One such is the fact that $E(x) \in \mathbb{Z}_p[[x]]$. That is, $E(x)$ turns out to be a power series in $\mathbb{Z}_p$! This property is known as integrality. In order to prove this, we need the following Lemmas (one of which is Dwork's Lemma):

Lemma (Dwork's lemma)

Let $f(x) \in 1 + x\mathbb{Q}_p[[x]]$ be a formal power series with p-adic rational coefficients. Then $f(x) \in 1 + x\mathbb{Z}_p[[x]] \iff \frac{f(x^p)}{f(x)^p} \in 1 + px\mathbb{Z}_p[[x]]$

Artin-Hasse Exponential Function

Lemma

$\exp(-px) \in 1 + p\mathbb{Z}_p[[x]]$

Lemma

$\frac{E(x^p)}{E(x)^p} = \exp(-px)$

These 3 Lemmas imply that $E(x) \in \mathbb{Z}_p[[x]]$.

Proposition

The radius of convergence of $E(x)$ is 1

For fun, if we have a finite extension of $\mathbb{Q}_p$, say $\mathbb{Q}_p(\sqrt{-p})$, does $E(\sqrt{p})$ converges? $E(\frac{1}{\sqrt{p}})$ converges? What do you think will be the radius of convergence of $E(x)$ in $\mathbb{Q}_p(\sqrt{-p})$ be?

Research Part of Artin-Hasse Exponential Function

Theorem (Lindemann)

Let $\alpha \in \mathbb{C}$ be algebraic $\implies \exp(\alpha)$ is transcendental. True for $\alpha \in \mathbb{Z}_p$ in the domain of the p-adic exponential.

It is not known if it is also true or false for $E(x)$! Now, let's reduce $E(x)$ $\bmod p$, and get $E_p(x) \in \mathbb{F}_p[[x]]$. Let $\mathbb{F}_p(x)$ be the field of rational functions over p, then it is not known whether $E(x)$ is algebraic over $\mathbb{F}_p(x)$. One motivation to prove this is the following theorem:

Theorem (Christol, 1979)

A formal power series $f(x) = \sum_{n \geqslant 0} b_n x^n \in \mathbb{F}_q[[x]]$ is algebraic over $\mathbb{F}_q(x)$ (field of rational functions) $\iff (b_n)$ is a q-automatic sequence.

Can you create a p-analogue for this q-automatic sequence from Christol?

Research Part of Artin-Hasse Exponential Function

Let $\overline{\mathbb{Q}_p}$ denote the algebraic closure of $\mathbb{Q}_p$. The algebraic closure of a field is an extension of the field in which every polynomial equation with coefficients in the field has a root in the extension. In simple terms, it adds all the missing algebraic solutions to polynomial equations.

We have the following theorem:

Theorem (Baker)

Let $\lambda \in \mathbb{C}$ be non-zero such that $\exp(\lambda) \in \overline{\mathbb{Q}_p}$. Then for any pair of rational numbers (a, b), not both zero, we have $a + b\lambda > H^{-C}$ (for some constant C, and H is the max height of (a, b))

The challenge is to formulate a p-analogue of this theorem.