An analogue of Hilbert’s tenth problem for fields of meromorphic functions over non-Archimedean valued fields

Xavier VIDAUX


Abstract

Let $K$ be a complete and algebraically closed valued field of characteristic 0. We prove that the set of rational integers is positive existentially definable in the field $\mathcal{M}$ of meromorphic functions on $K$ in the language $\mathcal{L}_z^*$ of rings augmented by a constant symbol for the independent variable $z$ and by a symbol for the unary relation “the function $x$ takes the value 0 at 0”. Consequently, we prove that the positive existential theory of $\mathcal{M}$ in the language $\mathcal{L}_z^*$ is undecidable. In order to obtain these results, we obtain a complete characterization of all analytic projective maps (over $K$) from an elliptic curve $\mathcal{E}$ minus a point to $\mathcal{E}$, for any elliptic curve defined over the field of constants.

This research was supported in part by the greek foundation of state scholarship (IKY) and was done at the university of Crete whose hospitality I acknowledge.
# Contents

1 Introduction 3

1.1 History - Setting of the problems 3

1.2 Main results - Related problems 4

1.3 Sketch of the proof 5

2 Rationality of analytic projective maps from an elliptic curve \( \mathcal{E} \) minus a point to \( \mathcal{E} \) 6

2.1 Relation between the speeds of convergence of the general term and of the partial sums of an ultrametric power series 6

2.2 Meromorphic functions on \( K - \{0\} \) 7

2.3 Extensions of Berkovich’s Theorem for elliptic curves 13

2.4 Rationality of global meromorphic solutions of Equation (MD) 14

2.5 Proof of Theorem A 19

3 Proof of Theorem B 21
Notation: The letter $K$ will denote a complete and algebraically closed valued field of characteristic 0 and the letter $\mathcal{M}$ will denote the field of meromorphic functions on $K$, of the variable $z$. By $\mathcal{L}_z$ we will denote the language of rings augmented by a constant symbol for the variable $z$, and by $\mathcal{L}_z^*$ we will denote the augmentation of $\mathcal{L}_z$ by a symbol for the unary relation “ord$_0(x) > 0$” (i.e.: the function $x$ takes the value 0 at 0).

1 Introduction

1.1 History - Setting of the problems

Hilbert’s tenth problem asked for an algorithm which decides, for any given Diophantine equation (polynomial equation in several variables with integer coefficients), whether the equation has or does not have integer solutions. Y. Matiyasevich proved in 1970 that Hilbert’s tenth problem has a negative answer (see [5, 17]). In the terminology of mathematical logic, the positive existential theory of the ring $\mathbb{Z}$ of rational integers is undecidable (see [4]).

The analogue of Hilbert’s tenth problem for the field $\mathbb{Q}$ of rational numbers is still an open problem. The first analogues of Hilbert’s tenth problem for rings other than the ring of rational integers were obtained by J. Denef (see, for instance, [7]). He obtained undecidability results for various rings of algebraic integers (e.g.: $\mathbb{Z}[i]$).

Extensions to rings or fields of functions:
The language $\mathcal{L}_z$ is a natural language in which one may consider problems analogous to Hilbert’s tenth problem for rings of functions of the variable $z$. Let $R$ be such a ring. The analogue of Hilbert’s tenth problem for $R$ in the language $\mathcal{L}_z$ is the following:

Is there an algorithm which, given any finite system of polynomial equations

$$(f_i = 0)_{i=1,...,k}$$

where $f_i \in \mathbb{Z}[z,T_1,\ldots,T_n]$, determines whether the system has or does not have a solution in $R$?

If the answer is yes, then we say that the positive existential theory of $R$ is decidable, else it is undecidable. The similar problem for systems $(f_i = 0)_{i=1,...,k} \land g \neq 0$ which contain also inequalities is the question whether the existential theory of $R$ in $\mathcal{L}_z$ is decidable or undecidable. The decidability question for the existential theory of $R$ in $\mathcal{L}_z^*$ is the similar problem where one allows the addition to the system of conditions of relations of the form ord$_0(x) > 0$, which are interpreted as “the function $x$ takes the value 0 at $z = 0$”.

A natural language in which one may consider questions of decidability is $\mathcal{L}_{z,C}$ which results from the augmentation of $\mathcal{L}_z$ by the predicate $C(x)$ for “$x$ is a constant”. In the following tables, we list some results about some rings of interest (if not specified, in the language $\mathcal{L}_{z,C}$). We denote by $\mathcal{A}(X)$ the ring of functions, analytic on an open set containing the set $X$ and by $\mathcal{M}(X)$ the field of fractions of $\mathcal{A}(X)$. By $\mathcal{U}$ we denote the unit disc (with or without boundary), and by $a$ an element of $X$. 

3
Complex case:

<table>
<thead>
<tr>
<th></th>
<th>( \mathbb{C}[z] )</th>
<th>( \mathbb{C}(z) )</th>
<th>( \mathcal{A}(\mathbb{C}) )</th>
<th>( \mathcal{M}(\mathbb{C}) )</th>
<th>( \mathcal{A}(\mathbb{U}) )</th>
<th>( \mathcal{A}({a}) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>ex. th. in ( \mathcal{L}^*_z )</td>
<td>und.</td>
<td>und.</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>

The existential decidability of the ring \( \mathcal{A}(\{a\}) \) is a consequence of [14, §7, Thm. 3]. The same theorem implies the analogous result in the \( p \)-adic case.

L. Rubel, in [22], proves that the positive existential theory of \( \mathcal{A}(\mathbb{U}) \), in the language of rings augmented by a symbol for the relation “\( x \) is not a constant”, is decidable. No analogue of this result is known for the \( p \)-adic case. Some other relevant results can be found in [13, 25, 26].

Non-Archimedean case:

The following table lists the analogous state of affairs in the \( p \)-adic case. We denote by \( \mathbb{C}_p \) the completion of an algebraic closure of the field of \( p \)-adic numbers. By \( \mathcal{A}_p(X) \) and \( \mathcal{M}_p(X) \) we denote respectively the ring of analytic functions and the field of meromorphic functions on the disc \( X \subset \mathbb{C}_p \).

<table>
<thead>
<tr>
<th></th>
<th>( \mathbb{C}_p[z] )</th>
<th>( \mathbb{C}_p(z) )</th>
<th>( \mathcal{A}_p(\mathbb{C}_p) )</th>
<th>( \mathcal{M}_p(\mathbb{C}_p) )</th>
<th>( \mathcal{A}_p(\mathbb{U}) )</th>
<th>( \mathcal{A}_p({a}) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>ex. th. in ( \mathcal{L}^*_z )</td>
<td>und.</td>
<td>und.</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>

The decidability result for the positive existential theory of \( \mathcal{A}(\{a\}) \) and \( \mathcal{A}_p(\{a\}) \) follows from [10, 11] and Artin’s approximation (see [1] and [18, Sect. 7]). No relevant results are known for the fields of fractions \( \mathcal{M}(\mathbb{U}) \), \( \mathcal{M}(\{a\}) \), \( \mathcal{M}_p(\mathbb{U}) \) and \( \mathcal{M}_p(\{a\}) \) in any of the languages \( \mathcal{L}_z \), \( \mathcal{L}^*_z \) or \( \mathcal{L}_{z,C} \).

We also note that the power series rings \( \mathbb{C}[[z]] \) and \( \mathbb{C}_p[[z]] \), as well as their field of fractions \( \mathbb{C}(z) \) and \( \mathbb{C}_p(z) \), have decidable theories in \( \mathcal{L}_{z,C} \) (see [14]). The ring \( \mathbb{C}[[z,w]] \) of power series in two variables has an undecidable full theory in \( \mathcal{L}_{z,C} \cup \{w\} \) (see [6]).

Finally, observe that the existential theories of \( \mathcal{A}(\{a\}) \) and \( \mathcal{A}_p(\{a\}) \) are undecidable in the language of rings augmented by a symbol \( \frac{d}{dz} \) for the derivation, since one can define the integers by an existential formula:

\[
    c \in \mathbb{Z} \iff \exists x(x \neq 0 \land c \frac{dx}{dz} = x).
\]

In this paper we prove the undecidability of the positive existential theory of the field \( \mathcal{M}_p(\mathbb{C}_p) \), in the language \( \mathcal{L}^*_z \). This result follows from Theorem B (see below).

1.2 Main results - Related problems

Let us give a few comments on our choice of the language \( \mathcal{L}^*_z \). Here we deal with solving systems of the form

\[
    P_i(f_1, \ldots, f_k) = 0, \quad \text{ord}_0(f_j) > 0, \quad i = 1, \ldots, n \quad \text{and} \quad j = 1, \ldots, k
\]
where \( P_i \) for \( i = 1, \cdots, n \), are polynomials with coefficients in \( \mathbb{Z}(z) \), and the variables \( f_1, \ldots, f_k \) range in \( \mathcal{M} \). One may consider that we deal with systems of differential equations “of order zero”, together with initial conditions (\( \text{ord}_0(f_j) > 0 \)). From this point of view, the language \( \mathcal{L}_z^* \) is of wide use in everyday mathematical practice. Of course it would be preferable to obtain the analogue of our theorem (see below) in the language \( \mathcal{L}_z \). However, the problem of defining existentially the relation \( \text{ord}_0(f) > 0 \) in the language \( \mathcal{L}_z \) over a field of functions is in general not trivial. In particular the problem is open for \( \mathbb{C}(z) \) as well as for the field of complex meromorphic functions (see [18, §2.5]).

We prove the following theorems:

**Theorem A** Let \( K \) be a complete algebraically closed valued field of characteristic \( 0 \). Let \( \mathcal{E} \) be an elliptic curve defined over \( K \) and let \( P \in \mathcal{E} \). Any analytic projective map (over \( K \)) on \( \mathcal{E} - \{P\} \) and into \( \mathcal{E} \) is rational.

Theorem A contrasts sharply the complex case in which there are many non-rational analytic projective maps from \( \mathcal{E} - \{P\} \) into \( \mathcal{E} \).

**Theorem B** Let \( K \) be a complete algebraically closed valued field of characteristic \( 0 \) and \( \mathcal{M} \) the field of meromorphic functions on \( K \). Let \( \mathcal{L}_z^* \) be the language of rings augmented by a constant symbol for the variable \( z \) and by a symbol for the unary relation \( \text{ord}_0(x) > 0 \) (i.e.: the function \( x \) takes the value 0 at 0).

(a) The set \( \mathbb{Z} \) of rational integers is positive existentially definable in \( \mathcal{M} \), in \( \mathcal{L}_z^* \).

(b) The positive existential theory of \( \mathcal{M} \) in \( \mathcal{L}_z^* \) is undecidable.

Fact (a) of Theorem B implies Fact (b) by Matiyasevich’s Theorem. A consequence of our result is the similar result for global analytic functions, in the language \( \mathcal{L}_z \), which was proved before (see [16]). The analogue of Theorem B in the language \( \mathcal{L}_z \), as well as the analogue for the field \( \mathcal{M}(D) \) of meromorphic functions on a disc \( D \), are open problems. The analogue of Theorem B for complex meromorphic functions is also open.

### 1.3 Sketch of the proof

We obtain Theorems A and B by proving that equations of the form

\[
(z^3 + \delta z^2 + z)y^2 = x^3 + \delta x^2 + x
\]

where \( z \) is the independent variable, have only rational solutions over \( \mathcal{M} \) (Theorem 2.22), for \( \delta \in K - \{\pm 2\} \). This result together with the fact that elliptic curves over \( K \) cannot be parametrized by global meromorphic functions (see Theorem 2.11) implies Theorem A. Theorem B follows from Theorem A (actually from the weaker Theorem 2.22) by techniques developed by J. Denef in [8].

In order to prove Theorem 2.22, we do as follows: let \( \mathcal{E} \) be the elliptic curve

\[
Y^2 = X^3 + \delta X^2 + X
\]

(1)
and let \( s \) be such that \( s^2 = z^3 + \delta z^2 + z \). A pair \((x, y) \in M^2\) is a solution of Equation (MD) if and only if \((x, sy)\) is a solution of \((1)\). The rational solutions of Equation (MD) are of the form \((x_n, y_n)\) where \((z, s) \mapsto (x_n(z), sy_n(z))\) is the \(n\)-th endomorphism of \(E\), for \(n \neq 0\). For any endomorphism \(n \neq 0\) of \(E\), we have the property

\[
x_{2n}(z^{-1}) = x_{2n}(z) \quad \text{and} \quad x_{2n+1}(z^{-1}) = x_{2n+1}(z).
\]

Now let \((x, y)\) be a solution of Equation (MD) over \(M\). We consider the map \(\tau\) defined by

\[
\tau(x, sy) = (x(z^{-1}), -\frac{s}{z^2}y(z^{-1}))
\]

and we look at the quantity \((\bar{x}, s\bar{y}) = (x, sy) \ominus \tau(x, sy)\) in order to understand how close a solution over \(M\) is to having the mentioned property of rational solutions. It will turn out that \((\bar{x}, s\bar{y})\) is a point of order 1 or 2 on \(E\). From this result, we will have enough information on \(x\) and \(y\) to conclude that they have to be rational (see Sect. 2.4).

In order to see that the quantity \((\bar{x}, s\bar{y})\) has to be a point of order 1 or 2, we investigate the solutions of Equation (MD) over the field \(M^\ast\) of functions which are meromorphic on \(K^\ast = K \setminus \{0\}\). For this purpose, crucial are the results of Sect. 2.1 and 2.2.

## 2 Rationality of analytic projective maps from an elliptic curve \(E\) minus a point to \(E\)

### 2.1 Relation between the speeds of convergence of the general term and of the partial sums of an ultrametric power series.

In what follows, we denote by \(|\cdot|\) the ultrametric absolute value of the field \(K\). Since the field \(K\) is complete, a power series in \(K[[T]]\) converges if and only if its general term converges to zero. The following proposition gives a relation between the speed of convergence of the general term and the speed of convergence of the partial sums of a given numerical series. First observe that if \(H = \sum_{n \geq 0} h_n\) is a convergent series, then the set \(|\{h_n|\ n \in \mathbb{N}\}|\) has a maximum.

**Proposition 2.1** Let \((h_n)_{n \geq 0}\) be a sequence of elements of \(K\) such that \(\sqrt[n]{|h_n|}\) converges to 0 as \(n\) goes to infinity. Let \(S_n\) denote the sequence \(\sum_{i=0}^{n} h_i\). Then \(S = \sum_{i \geq 0} h_i\) exists and the sequence \(\sqrt[n]{|S_n - S|}\) converges to 0 as \(n\) goes to infinity.
Proof: Clearly the limit $S$ of $S_n$ exists. For any integer $n$, we have:

$$\sqrt{|S_n - S|} = \sqrt{n \left| \sum_{i \geq n+1} h_i \right|} \\
\leq \sqrt{n \max_{i \geq n+1} |h_i|} \\
= \sqrt{n \max_{j \geq 1} |h_{n+j}|} \\
= \sqrt{|h_{n+j_0}|} \\
= \left( n^{\frac{j_0}{2}} \sqrt{|h_{n+j_0}|} \right)^{\frac{1}{n}} \xrightarrow{n \rightarrow \infty} 0$$

for some integer $j_0 \geq 1$. Note that the integer $j_0$ depends a priori on $n$, but only the fact that it is positive matters.

Corollary 2.2 Let $\sum h_n T^n$ be a power series in $K[[T]]$ with infinite radius of convergence, such that $\sum h_n = S$, and let $S_n$ denote the partial sum $\sum_{i=0}^n h_i$. Then the power series $\sum (S_n - S) T^n$ has infinite radius of convergence.

Actually we can obtain something better (this is what we will need later on):

Lemma 2.3 For any integers $n$ and $k$, let $c_{n,k}$ be an element of the valuation ring of $K$ (that is $|c_{n,k}| \leq 1$). Assume that $(h_n)_{n \geq 0}$ is a sequence of elements of $K$ such that $\sqrt{|h_n|}$ converges to 0 as $n$ goes to infinity. For each $n$, let $R_n$ denote the sequence

$$\sum_{k \geq n} c_{n,k} h_k.$$

Then the sequence $\sqrt{|R_n|}$ converges to 0.

Proof: Note that if the $c_{n,k}$ are all 1, then we obtain Proposition 2.1, setting $R_n = S - S_{n-1}$. The proof of the generic case is similar to that of Proposition 2.1 and is left to the reader.

2.2 Meromorphic functions on $K - \{0\}$

We refer to [12], [15], or [20] for the following definitions and basic facts. A function $h$ is analytic on $K$ if there exists a formal power series $\sum_{n \in \mathbb{N}} h_n T^n \in K[[T]]$ converging everywhere in $K$ such that, for all $z \in K$, we have $h(z) = \sum_{n \in \mathbb{N}} h_n z^n$. We will say that a function is meromorphic on $K$ if it can be written as the quotient of two analytic functions on $K$. Let $K^*$ denote the set $K - \{0\}$. A function $h$ is analytic on $K^*$ if there exists a formal Laurent series $\sum_{n \in \mathbb{Z}} h_n T^n \in K[[T,T^{-1}]]$ converging everywhere in $K^*$ such that, for all $z \in K^*$, we have $h(z) = \sum_{n \in \mathbb{Z}} h_n z^n$. We will say that a function is meromorphic on $K^*$ if it can be written as the quotient of two analytic functions on $K^*$. Analytic (resp. meromorphic) functions on $K$ will be called also global analytic functions (over $K$) (resp. global meromorphic functions (over $K$)).
The integral domain of analytic functions on $K$ (resp. on $K^*$) will be denoted by $A$ (resp. by $A^*$) and the field of fractions of $A$ (resp. of $A^*$) will be denoted by $M$ (resp. by $M^*$).

We will gather what we need in the following lemma. The order of a zero or a pole of a meromorphic function is well defined. See [20, chap.6, p. 305], for a proof of this fact and of the following.

**Lemma 2.4**

1. A meromorphic function $f$ in $M$ or in $M^*$ has no accumulation of poles and, if $f \neq 0$, then $f$ has no accumulation of zeros.

2. A global analytic function either is a polynomial or has infinitely many zeros.

3. A global meromorphic function avoids at most one value, in which case it can be written as $C + \frac{1}{h}$ where $C$ is the avoided value and $h$ is a global analytic function.

4. A meromorphic function without any pole is an analytic function.

5. A global meromorphic function having finitely many zeros and finitely many poles is a rational function.

6. If a global meromorphic function has infinitely many zeros (resp. poles), then they can be arranged as a sequence of zeros (resp. poles) whose absolute value goes to infinity.

7. Meromorphic functions in $M$ or in $M^*$ can be written as the quotient of two analytic functions with no common zeros.

We will say that a function $f : K^* \to K$ is invariant under the map $z \mapsto z^{-1}$ if, for any $z$ in $K^*$, we have $f(z) = f(\frac{1}{z})$.

**Lemma 2.5** Let $h$ and $f$ be two meromorphic functions on $K$. If for every non-zero $z$ in $K$, we have $h(z) = f(z^{-1})$, then the functions $h$ and $f$ are rational functions. If the functions $h$ and $f$ are analytic functions on $K$, then they are constant.

*Proof:* Observe that if $\varrho \neq 0$ is a zero (resp. a pole) of $h$, then $\frac{1}{\varrho}$ is a zero (resp. a pole) of $f$. Assume that $h$ has infinitely many zeros (resp. poles). Then it has a sequence $\varrho_n$ of zeros (resp. poles) whose absolute value converges to infinity. Then the sequence $\frac{1}{\varrho_n}$ is a sequence of zeros (resp. poles) of $f$ whose absolute value converges to 0, and this is not possible. Consequently the function $h$, therefore $f$ as well, has finitely many zeros and finitely many poles. So they must be rational functions. This finishes the proof of the first assertion. The second assertion is then easy and is left to the reader. 

The next lemma is a consequence of the uniqueness of the expansion of analytic functions on $K^*$ (see [15]).

**Lemma 2.6** Let $h = \sum_{n \in \mathbb{Z}} a_n z^n$ be a non-zero analytic function on $K^*$, invariant under $z \mapsto z^{-1}$. Then for all $n \in \mathbb{Z}$ we have $a_n = a_{-n}$.
Lemma 2.7 Let $h \neq 0$ be a function in $\mathcal{A}^*$. Then $h$ can be written as
\[
h(z) = Cz^m \prod_{|\rho| \geq 1} \left(1 - \frac{z}{\rho}\right)^{\nu_\rho} \prod_{|\rho| < 1} \left(1 - \frac{\rho}{z}\right)^{\nu_\rho},
\]
the products being taken over all non-zero zeros $\rho$ of $h$, the integer $\nu_\rho$ being the multiplicity of $h$ at $\rho$.

Proof: See [20, chap. 6, p. 320].

Lemma 2.8 Let $h$ be an analytic function on $K^*$, invariant under $z \mapsto z^{-1}$. Then there exists a unique function $g$, analytic on $K$, such that for all $z$ in $K^*$, $g$ satisfies
\[
h(z) = g(z + z^{-1})
\]

Proof: Let us write $w = z + z^{-1}$. By lemma 2.6, we have:
\[
h(z) = a_0 + \sum_{n \geq 1} a_n z^n + \sum_{n \geq 1} a_n z^{-n}
\]

Fix an integer $N \geq 1$. Let us write
\[
h_N(z) = a_0 + \sum_{n=1}^N a_n z^{-n} + \sum_{n=1}^N a_n z^n
\]

Clearly, the function $h_N(z)$ is a polynomial in $w$ of degree at most $N$. Let us write this polynomial as
\[
G_N(w) = \sum_{n=0}^N b_{n,N} w^n
\]

If there exists an integer $N_0$ such that, for any integer $n > N_0$, we have $a_n = 0$, then $h_{N_0} = h$, and in this case, the polynomial $G_{N_0}$ is the function $g$ we are looking for. From now on, we will suppose that infinitely many $a_n$ are not 0.

The proof is done in three steps. First, for $N$ fixed, we will express $b_{n,N}$ as a linear combination of the $a_n$’s with integer coefficients, and this will imply that, for any fixed integer $n$, the sequence $b_{n,N}$ converges as $N$ goes to infinity. We will write $b_n = \lim_{N \to +\infty} b_{n,N}$. Secondly, we will prove that the function $g$ defined by the power series $\sum_{n=0}^\infty b_n T^n$ is an analytic function on $K$. Finally, we will prove that this function satisfies $g(z + z^{-1}) = h(z)$. In other words, we will find the function $g$ by successive approximation of the coefficients of its power series expansion.

Fix the integer $N$. Let $k$ be any non-negative integer such that $n + 2k \leq N$. Write:
\[
(z + z^{-1})^{n+2k} = \sum_{j=0}^{n+2k} \binom{n+2k}{j} z^{n+2k-j} z^{-j} = \sum_{j=0}^{n+2k} \binom{n+2k}{j} z^{n+2k-2j}
\]
We observe that, on the right hand side of the equation, the term \( z^n \) corresponds to \( j = k \) and the term \( z^{-n} \) corresponds to \( j = n + k \). Then the coefficient of \( z^n \) is \( \binom{n + 2k}{k} \) and the coefficient of \( z^{-n} \) is \( \binom{n + 2k}{n + k} \). Also observe that
\[
\binom{n + 2k}{k} = \binom{n + 2k}{n + k}
\]
Since the coefficients of \( z^n + z^{-n} \) in \( h_N(z) \) and \( G_N(z + z^{-1}) \) must be equal, we see that the unknowns \( b_{n,N} \) satisfy the following system of \( N + 1 \) equations:
\[
(S^N) \quad a_n = \sum_{k=0}^{\lfloor \frac{N-n}{2} \rfloor} \binom{n + 2k}{k} b_{n+2k,N}, \quad \text{for } n = 0, \ldots, N,
\]
where \( [x] \) denotes the integral part of \( x \). This is a triangular system of \( N + 1 \) equations and \( N + 1 \) unknowns (the \( b_{n+2k,N} \)). We obtain \( b_{N,N} \) from the equation \( a_N = b_{N,N} \), we obtain \( b_{N-1,N} \) from the equation \( a_{N-1} = \binom{N-1}{0} b_{N-1,N} \), and we obtain \( b_{n,N} \) from
\[
a_n = \binom{n}{0} b_{n,N} + \binom{n + 2}{1} b_{n+2,N} + \cdots
\]
Observe that since \( \binom{n}{0} = 1 \), we have
\[
b_{n,N} = \sum_{k=n}^{N} c_{n,N,k} a_k
\]
for some rational integers \( c_{n,N,k} \). These \( c_{n,N,k} \) depend a priori on \( N \). In order to see that they are actually independent of \( N \), we treat \( a_n \) and \( b_n \) as variables, we consider the expression of \( a_n \) in the systems \( S^N \) and \( S_{N+2} \), and we subtract them:
\[
0 = a_n - a_n
\]
\[
= \sum_{k=0}^{\lfloor \frac{N-n}{2} \rfloor} \binom{n + 2k}{k} b_{n+2k,N+2} - \sum_{k=0}^{\lfloor \frac{N-n}{2} \rfloor} \binom{n + 2k}{k} b_{n+2k,N}
\]
\[
= \sum_{k=0}^{\lfloor \frac{N-n}{2} \rfloor} \left( \binom{n + 2k}{k} (b_{n+2k,N+2} - b_{n+2k,N}) \right) + \binom{N+2}{\lfloor \frac{N+2}{2} \rfloor} b_{N+2,N+2}
\]
For \( n = N \), we obtain \( k = 0 \) and
\[
0 = b_{N,N+2} - b_{N,N} + \binom{N+2}{1} b_{N+2,N+2}
\]
that is
\[
b_{N,N+2} - b_{N,N} = -\binom{N+2}{1} a_{N+2}
\]
By downwards induction \( (n = N-2, \ldots) \), we have, for any integer \( n \) such that \( 0 \leq n \leq N \),
\[
b_{n,N+2} - b_{n,N} = c \cdot a_{N+2}
\]
for some integer \( c \) depending on \( n \) and \( N \). This proves that \( a_k \), for \( k = n, \ldots, N \), appears with the same coefficient in \( b_{n,N} \) and in \( b_{n,N+2} \) and we conclude that the integers \( c_{n,N,k} \) do not depend on \( N \). So we can write \( c_{n,N,k} = c_{n,k} \), and then

\[
b_{n,N} = \sum_{k=n}^{N} c_{n,k} a_k
\]

Let us now fix the integer \( n \). Since \( h \) converges on \( K^* \), the sequence \( |a_k| \) converges to 0 as \( k \) goes to infinity. Since the coefficients \( c_{n,k} \) are integers, the sequence \( |c_{n,k}a_k| \) converges also to zero as \( k \) goes to infinity and then the sequence \( b_{n,N} \) converges as \( N \) goes to infinity; let \( b_n \) denote the limit of \( b_{n,N} \) as \( N \) goes to infinity, that is

\[
b_n = \sum_{k \geq n} c_{n,k} a_k
\]

Let \( g(T) \) denote the formal power series:

\[
g(T) = \sum_{n \geq 0} b_n T^n \in K[[T]]
\]

By Lemma 2.3, the power series \( g(T) \) has an infinite radius of convergence (apply Lemma 2.3 for \( h_k = a_k \) and \( R_n = b_n \)).

It remains to show that \( g(z + z^{-1}) = h(z) \) for any non-zero \( z \) in \( K \). Let us write:

\[
g_N(w) = \sum_{n=0}^{N} b_n w^n
\]

On the one hand, for any integer \( N \) and any \( z \in K^* \), we have

\[
G_N(z + z^{-1}) = h_N(z)
\]

and then, as \( N \) goes to infinity, \( G_N(z + z^{-1}) \) converges to \( h(z) \). On the other hand, \( g_N(z + z^{-1}) \) converges to \( g(z + z^{-1}) \) as \( N \) goes to infinity. So we have to prove that \( g_N(w) - G_N(w) \) converges to 0 as \( N \) goes to infinity. Fix an arbitrary \( N \). We have:

\[
|g_N(w) - G_N(w)| = \left| \sum_{n=0}^{N} b_n w^n - \sum_{n=0}^{N} b_{n,N} w^n \right|
\]

\[
\leq \max_{n=0} \left\{ |b_n - b_{n,N}| \cdot |w|^n \right\}
\]

\[
= \max_{n=0} \left\{ \left( \sum_{k \geq N+1} c_{n,k} a_k \right) \cdot |w|^n \right\}
\]

Let \( u(N) \) denote the integer \( n \) for which the maximum is reached. Observe that we have \( 0 \leq u(N) \leq N \). The inequality becomes:

\[
|g_N(w) - G_N(w)| \leq \sum_{k \geq N+1} c_{u(N),k} \cdot a_k \cdot |w|^{u(N)} = |R_{N+1}| \cdot |w|^{u(N)}
\]
where
\[ R_{N+1} = \sum_{k \geq N+1} c_{u(N), k} \cdot a_k \]
Apply Lemma 2.3 with \( n \) replaced by \( N + 1 \) and \( h_k \) replaced by \( a_k \), to obtain:

- If \( |w| < 1 \) then we have: \( |R_{N+1}| \cdot |w|^u(N) \xrightarrow{N \to \infty} 0 \)
- If \( |w| \geq 1 \) then we have \( |w|^u(N) \leq |w|^N \), and so
  \[ |R_{N+1}| \cdot |w|^u(N) \leq |R_{N+1}| \cdot |w|^N \]
By Lemma 2.3, we have \( N \sqrt{|R_{N+1}| \cdot |w|^N} \xrightarrow{N \to \infty} 0 \), thus
  \[ N \sqrt{|R_{N+1}| \cdot |w|^N} \xrightarrow{N \to \infty} 0 \]
which implies that
  \[ |R_{N+1}| \cdot |w|^N \xrightarrow{N \to \infty} 0 \]

The uniqueness of \( g \) is easily seen (by the fact that two distinct meromorphic functions cannot take the same value at each point of a set containing an accumulation point).

**Lemma 2.9** Let \( h \) be a meromorphic function on \( K^* \) invariant under the map \( z \mapsto z^{-1} \). There exist functions \( h_1 \) and \( h_2 \) analytic on \( K^* \) and invariant under \( z \mapsto z^{-1} \) such that
\[ h = h_1 h_2. \]

**Proof:** We use Lemmas 2.7 and 2.4. Let us write \( h \) as the quotient \( \frac{h_1}{h_2} \) of two functions in \( A^* \) with no common zeros. We can suppose without loss of generality that the factor \( z^m \) does not appear in the product expansion of \( h_2 \) (see Lemma 2.7, if \( m \neq 0 \), we multiply both \( h_1 \) and \( h_2 \) by \( z^{-m} \)). If \( \rho \) is any element of \( K^* \) and \( n \) a positive integer, \( \rho \) is a zero of order \( n \) of \( h_1 \) if and only if \( \rho \) is a zero of order \( n \) of \( h_1 \), which happens if and only if \( \frac{1}{\rho} \) is a zero of order \( n \) of \( h \), and this happens if and only if \( \frac{1}{\rho} \) is a zero of order \( n \) of \( h_1 \).

Let us write
\[ \pi(z) = \prod_{|\rho| = 1 \atop h_1(\rho) = 0} \left( 1 - \frac{z}{\rho} \right)^{\nu_\rho} \]
\[ \pi^+(z) = \prod_{|\rho| > 1 \atop h_1(\rho) = 0} \left( 1 - \frac{z}{\rho} \right)^{\nu_\rho} \quad \text{and} \quad \pi^-(z) = \prod_{|\rho| < 1 \atop h_1(\rho) = 0} \left( 1 - \frac{\rho}{z} \right)^{\nu_\rho} \]
By Lemma 2.7 we have, for some constant \( C \) and integer \( m \)
\[ (\star) \quad h_1(z) = C z^m \pi(z) \pi^+(z) \pi^-(z) \]
For an arbitrary \( \rho \neq 0 \), writing \( \rho = \frac{1}{\mu} \), we have seen that \( h_1(\rho) = 0 \) if and only if \( h_1(\mu) = 0 \) and \( \nu_\rho = \nu_\mu \). Then we have
\[ \pi(z) = \prod_{|\rho| = 1 \atop h_1(\rho) = 0} \left( 1 - \frac{z}{\rho} \right)^{\nu_\rho} = \prod_{|\rho| = 1 \atop h_1(\mu) = 0} \left( 1 - z\mu \right)^{\nu_\mu} = \pi(z^{-1}) \]
\[
\pi^+(z) = \prod_{\|\rho\| > 1, h_1(\rho) = 0} \left(1 - \frac{z}{\rho}\right)^{\nu_\rho} = \prod_{|\mu| > 1, h_1(\mu) = 0} (1 - z\mu)^{\nu_\mu} = \pi^-(z^{-1})
\]
and
\[
\pi^-(z) = \prod_{|\rho| < 1, h_1(\rho) = 0} \left(1 - \frac{\rho}{z}\right)^{\nu_\rho} = \prod_{|\mu| < 1, h_1(\mu) = 0} (1 - \frac{1}{z\mu})^{\nu_\mu} = \pi^+(z^{-1})
\]

Therefore we have
\[
\frac{h_1(z)}{Cz^m} = \pi(z)\pi^+(z)\pi^-(z) = \pi(z^{-1})\pi^-(z^{-1})\pi^+(z^{-1}) = \frac{h_1(z^{-1})}{Cz^{-m}}
\]
which implies that
\[
h_1(z^{-1}) = z^{-2m}h_1(z)
\]

We prove in the same way that \(h_2(z^{-1}) = h_2(z)\) (we do not have for \(h_2\) the factor \(z^m\) because we have supposed that \(z\) does not divide \(h_2\)). Thus we have
\[
h(z) = h(z^{-1}) = \frac{h_1(z^{-1})}{h_2(z^{-1})} = \frac{z^{-2m}h_1(z)}{h_2(z)} = z^{-2m}h(z),
\]
which implies that \(m = 0\).

Corollary 2.10 Let \(h\) be a meromorphic function on \(K^*\) invariant under \(z \mapsto z^{-1}\). Then there exists a function \(g\) in \(M\) such that, for all \(z\) in \(K^*\), \(g\) satisfies \(h(z) = g(z + z^{-1})\).

Proof: By Lemma 2.9, \(h\) can be written as \(\frac{h_1}{h_2}\), for some functions \(h_1\) and \(h_2\) in \(A^*\) invariant under \(z \mapsto z^{-1}\). By lemma 2.8, there exist functions \(g_1\) and \(g_2\) in \(A\) such that, for all \(z \in K^*\), \(h_1(z) = g_1(z + z^{-1})\) and \(h_2(z) = g_2(z + z^{-1})\). Writing \(g = \frac{g_1}{g_2} \in M\), we have \(h(z) = g(z + z^{-1})\).

2.3 Extensions of Berkovich’s Theorem for elliptic curves

From now on the letter \(F\) denotes the polynomial \(T^3 + \delta T^2 + T\).

Theorem 2.11 (Berkovich) Let \(x\) and \(y\) be two meromorphic functions on \(K\) which satisfy Equation (1), that is,
\[
y^2 = x^3 + \delta x^2 + x
\]

Then \(x\) and \(y\) are constant.

Proof: See [2, Chap. 4, Thm. 4.5.1] for a proof of a more general result; [3, Cor. A, p. 753] for a proof involving \(p\)-adic Nevanlinna’s theory; or [24, Sect. 8] for a proof using a characterization of non-global solutions of (1).

Theorem 2.12 Let \(x\) and \(y\) be two meromorphic functions on \(K^*\), invariant under \(z \mapsto z^{-1}\), which satisfy Equation (1), that is,
\[
y^2 = x^3 + \delta x^2 + x
\]

Then \(x\) and \(y\) are constant.
Proof: By Corollary 2.10, there exist functions $g_1$ and $g_2$ in $\mathcal{M}$ such that, for all $z \in K^*$, $x(z) = g_1(z + z^{-1})$ and $y(z) = g_2(z + z^{-1})$. It is obvious that $(g_1, g_2)$ satisfies the same equation as $(x, y)$. Thus by Berkovich’s Theorem, $g_1$ and $g_2$ must be constant. Therefore, $x$ and $y$ must be constant. \hfill \diamond

**Theorem 2.13** Let $x$ and $y$ be two meromorphic functions on $K^*$, invariant under $z \mapsto z^{-1}$, which satisfy

$$(z + \delta + z^{-1})y^2 = x^3 + \delta x^2 + x$$

Then $(x, y)$ is a point of order 2 of $\mathcal{E}$.

Proof: Write $w = z + z^{-1}$. We know by Corollary 2.10 that there exist global meromorphic functions $g$ and $h$ such that $x(z) = g(w)$ and $y(z) = h(w)$. Then, in terms of the variable $w$, our equation becomes

$$(w + \delta)h^2 = F(g)$$

Set $w = t^2 - \delta$, then the equation becomes

$$(t \cdot h \circ (t^2 - \delta))^2 = F(g \circ (t^2 - \delta))$$

and we can conclude by Berkovich’s Theorem that both functions $t \cdot h \circ (t^2 - \delta)$ and $g \circ (t^2 - \delta)$ are constant. Since $h \circ (t^2 - \delta) = a \text{ constant}$ as a function of $t$, both even and odd, the constant must be zero. Since $t^2 - \delta$ is surjective ($K$ is algebraically closed), we conclude that $h = 0$, and then $y = 0$. Then $F(x) = 0$, and so $x$ can take only three values, those corresponding to the roots of the polynomial $F$. Thus $x$ is constant. Finally, we obtain that $(x, y)$ is one of the three points of order 2 of $\mathcal{E}$: $(0, 0)$, $(\xi, 0)$ or $(\xi^{-1}, 0)$, where $\xi$ is one of the non-zero roots of the polynomial $F$. \hfill \diamond

### 2.4 Rationality of global meromorphic solutions of Equation (MD)

We will study now equations of the form

(\text{MD}) \hspace{1cm} (z^3 + \delta z^2 + z)y^2 = x^3 + \delta x^2 + x

where $z$ is the independent variable, $x$ and $y$ are functions of $z$. We fix a $\delta \in K - \{\pm 2\}$, so that Equation (MD) defines an elliptic curve $\mathcal{E}^\ast$. These curves have been introduced by Y. Manin and J. Denef. We show that Equation (MD) has only rational solutions over $\mathcal{M}$ (see Theorem 2.22).

**Remark 2.14** Let us consider, over any field, a solution $(x, y)$ of Equation (MD):

$$F(z)y^2 = F(x)$$

Let $s$ be an element of an algebraic closure of $K(z)$ such that $s^2 = F(z)$. Then $(x, sy)$ is a point on the elliptic curve $\mathcal{E}$ (it is a solution of Equation (1)). From now on, $(x, sy)$ is both a point on $\mathcal{E}$, considered as an elliptic curve over $\mathcal{M}$, and a map from $\mathcal{E} - \{\infty\}$ to $\mathcal{E}$:

$$(z, s) \mapsto (x(z), sy(z))$$
Let us fix a solution \((x, y)\) of Equation (MD) over the field \(\mathcal{M}\). Observe that the composition of elements of \(\mathcal{M}\) is not, in general, in \(\mathcal{M}\). But considering a function \(h\) in \(\mathcal{M}\) as a meromorphic function on \(K^*\), we can compose it with the function of \(\mathcal{M}^*\) which sends \(z\) to \(z^{-1}\); the function \(h \circ (z^{-1})\) still lies in \(\mathcal{M}^*\).

The map \(\iota: z \mapsto z^{-1}\) is, obviously, an automorphism over \(K\) of the field \(K(z)\) of rational functions. This automorphism \(\iota\) extends to an automorphism of the field extension \(K(z, s)\) of \(K(z)\) in two ways. Since

\[
\iota(s^2) = \iota(F(z)) = F(z^{-1}) = \frac{1}{z^4}F(z) = \frac{s^2}{z^4},
\]

\(s\) may be mapped to any of \(\pm \frac{s}{z^2}\). Let \(\tilde{\iota}\) denote the automorphism of \(K(z, s)\) which sends \(s\) to \(-\frac{s}{z^2}\). Observe that, under composition, \(\tilde{\iota} \circ \tilde{\iota}\) is the identity function.

If \((z, s) \in \mathcal{E}(K^*)\), then the pair \((\tilde{\iota}(z), \tilde{\iota}(s))\) lies in \(\mathcal{E}(K^*)\). Therefore, to \(\tilde{\iota}\) corresponds naturally a map \(\tau_0: \mathcal{E}(K^*) \rightarrow \mathcal{E}(K^*)\), which sends the point \((z, s)\) to

\[
(\tilde{\iota}(z), \tilde{\iota}(s)) = (z^{-1}, -\frac{s}{z^2}).
\]

Obviously, the map \(\tau_0\) is of order 2, that is \(\tau_0 \circ \tau_0\) is the identity of \(\mathcal{E}(K^*)\). Let \(\tau: \mathcal{E}(\mathcal{M}) \rightarrow \mathcal{E}(\mathcal{M}^*)\) denote the map which sends the point \((x, sy)\) to

\[
(x \circ z^{-1}, -\frac{s}{z^2} y \circ z^{-1}) = (x, sy) \circ \tau_0
\]

Observe that, since \(\tau(x, sy)\) is a solution of Equation (1) over \(\mathcal{M}^*\), the image of the map \(\tau\) is included in \(\mathcal{E}(\mathcal{M}^*)\). Since the map \(\tau_0\) is of order 2, the map \(\tau\), also, is of order 2.

**Remark 2.15** Consider \((z, s)\) as a point on the elliptic curve \(\mathcal{E}\). Note that, by the addition law on \(\mathcal{E}\), we have

\[
(z, s) \oplus (0, 0) = (z^{-1}, -\frac{s}{z^2})
\]

Then, considering \((x, sy)\) as a function of the variable \((z, s)\), we could also define the map \(\tau\) by:

\[
\tau(x, sy) = (x, sy) \circ [(z, s) \oplus (0, 0)]
\]

If \(P\) is any point on the elliptic curve \(\mathcal{E}\) (over any field), we will write \(\pm P\) to mean that we consider either the point \(P\) or its opposite \(\ominus P\).

**Lemma 2.16** For any solution \((x, y)\) of Equation (MD), with \(x\) and \(y\) in \(\mathcal{M}^*\), we have:

1. \(\tau(2(x, sy)) = 2\tau(x, sy)\)
2. \(\tau(2(x, sy) \oplus (z, s)) = 2\tau(x, sy) \oplus \tau(z, s)\)
3. If \((x, sy) \neq \pm \tau(x, sy)\) then \(\tau((x, sy) \ominus \tau(x, sy)) = \tau(x, sy) \ominus (x, sy)\)

**Proof:** In order to simplify the formulae, we will write \(\tilde{x} = x \circ z^{-1}\) and \(\tilde{y} = y \circ z^{-1}\). See [23, Chap. III, p. 58] for the general algorithm giving the addition formula of an elliptic curve.
1. Write \((a, sb) = 2(x, sy)\) and \((u, v) = \tau(2(x, sy))\). By the addition law on \(E\), we have
\[
a = \left( \frac{3x^2 + 2\delta x + 1}{2sy} \right)^2 - \delta - 2x
\]
and
\[
sb = -\frac{(3x^2 + 2\delta x + 1)(x^2 - 1)^2 - 4s^2y^2(x^3 - x)}{8y^3s^3}
\]
So we have:
\[
u = \left( \frac{3\tilde{x}^2 + 2\delta \tilde{x} + 1}{-2\tilde{z}\tilde{y}} \right)^2 - \delta - 2\tilde{x}
\]
and
\[
v = -\frac{(3\tilde{x}^2 + 2\delta \tilde{x} + 1)(\tilde{x}^2 - 1)^2 - 4\tilde{x}^2\tilde{y}^2(\tilde{x}^3 - \tilde{x})}{-8\tilde{y}^3\tilde{s}^3}
\]
Therefore we have
\[
\tau(2(x, sy)) = 2(\tilde{x}, \frac{-s}{z^2}\tilde{y}) = 2\tau(x, sy)
\]

2. Write
\[
(a, sb) = 2(x, sy)
\]
\[
(u, v) = (a, sb) \oplus (z, s)
\]
\[
(t, w) = \tau((a, sb) \oplus (z, s))
\]
\[\tilde{a} = a \circ z^{-1} \quad \text{and} \quad \tilde{b} = b \circ z^{-1}\]. Note that \(a\) cannot be equal to \(z\), because \((z, s)\) cannot be written as the double of a solution (see Definition 2.18 and Lemma 2.19). We have
\[
u = \left( \frac{s - sb}{z - a} \right)^2 - \delta - z - a
\]
and
\[
v = -\left( \frac{s - sb}{z - a} \right) u(z, s) - \frac{sbz - as}{z - a}
\]
Therefore we have
\[
t = \left( \frac{-\frac{s}{z} + \frac{s}{z} \tilde{b}}{z^{-1} - \tilde{a}} \right)^2 - \delta - z^{-1} - \tilde{a}
\]
and
\[
w = -\left( \frac{-\frac{s}{z} + \frac{s}{z} \tilde{b}}{z^{-1} - \tilde{a}} \right) u(z^{-1}, -\frac{s}{z^2}) - \frac{-\frac{s}{z} \tilde{b} z^{-1} + \tilde{a} \frac{s}{z^2}}{z^{-1} - \tilde{a}}
\]
We conclude that
\[
(t, w) = (\tilde{a}, -\frac{s}{z^2}\tilde{b}) \oplus (z^{-1}, -\frac{s}{z^2}) = \tau(a, sb) \oplus \tau(z, s)
\]
Use 1, above, to obtain the result.
3. Write $(u, v) = (x, sy) \oplus \tau(x, sy)$. We have

$$u = \left( \frac{\frac{\delta - sy}{x} - \delta - x}{x - x} \right)^2 - \delta - x$$

and

$$v = -\frac{\frac{\delta - sy}{x} - \delta - x}{x - x} u - \frac{\delta - sy}{x - x} \frac{\delta - sy}{x - x}$$

Therefore the quantity $(u, v)$ becomes $(u, -v) = \ominus(u, v)$ if we change $z$ to $z^{-1}$ and $s$ to $\frac{s}{z^2}$, that is, if we apply the function $\tau$.

\[\Box\]

**Lemma 2.17** Assume that $x$ and $y$ are functions in $\mathcal{M}$ and $(x, y)$ is a solution of Equation (MD). Then, either $(x, sy) = \pm \tau(x, sy)$, or the point $(\bar{x}, \bar{y}) \in \mathcal{E}^{*}(\mathcal{M}^*)$ defined by

$$(\bar{x}, \bar{y}) = (x, sy) \ominus \tau(x, sy)$$

is a point of order 2 of $\mathcal{E}$.

**Proof:** Assume that $(x, sy) \neq \pm \tau(x, sy)$. Then the pair $(\bar{x}, \bar{y})$ satisfies Equation (MD), which we can write as

$$(z + \delta + \bar{y})(z\bar{y})^2 = F(\bar{x})$$

By Lemma 2.16 (3), we have

$$\tau(\bar{x}, \bar{y}) = \ominus(\bar{x}, \bar{y})$$

Then, by the definition of $\tau$, for any $(z_0, s_0) \in \mathcal{E}(K)$, with $z_0 \neq 0$, we have $\bar{x}(z_0^{-1}) = \bar{x}(z_0)$ and

$$\frac{s_0 - s_0}{z_0^2} \bar{y}(z_0^{-1}) = -s_0 \bar{y}(z_0)$$

that is $\bar{y}(z_0^{-1}) = \frac{s}{z^2} \bar{y}(z_0)$. The latter implies that the function $z\bar{y}$ is invariant under $z \mapsto z^{-1}$. We then apply Theorem 2.13 to the pair $(\bar{x}, \bar{y})$ to obtain the conclusion. \[\Box\]

**Definition 2.18** We will call a global meromorphic solution $(x, y)$ of Equation (MD) **even** (resp. **odd**) if there exists a global meromorphic solution $(a, b)$ of Equation (MD) such that $(x, sy) = 2(a, sb)$ (resp. $(x, sy) = 2(a, sb) \oplus (z, s)$). We will say also that $(x, sy)$ is **even** (resp. **odd**) if $(x, y)$ is even (resp. odd). We will say that a solution $(x, y)$ of Equation (MD) has the even property, if $(x, y)$ satisfies:

$$x(z^{-1}) = x(z) \quad \text{and} \quad y(z^{-1}) = \pm z^2 y(z).$$

We will say that a solution $(x, y)$ of Equation (MD) has the odd property, if $(x, y)$ satisfies:

$$x(z^{-1}) = x^{-1}(z) \quad \text{and} \quad y(z^{-1}) = z^2 \frac{y}{x^2}.$$

**Lemma 2.19** A point of order 2 on $\mathcal{E}$ is not an even solution. A non-trivial solution cannot be both even and odd.
Proof: The proof is easy and is left to the reader.

The next Corollary is not necessary for proving Theorem 2.22. We present it nevertheless because it gives a nice correspondence between two kinds of properties of the solutions of Equation (MD). Note that Corollary 2.20 was known for rational solutions. Our proof does not use rationality. This amazing property of rational solutions was the starting point of our investigation.

Corollary 2.20 If \((x, y)\) is an even (resp. odd) global meromorphic solution of Equation (MD), then \((x, y)\) has the even (resp. odd) property.

Proof: If \((x, sy)\) is even, then by Lemma 2.16 (1), \(\tau(x, sy)\) is also even. If \((x, sy)\) were not equal to \(\pm \tau(x, sy)\), then the pair \((\bar{x}, s\bar{y})\) defined in Lemma 2.17 would be even, which is impossible by Lemma 2.19. Then we are in the case \((x, sy) = \pm \tau(x, sy)\). Now from this equality, we obtain that the pair \((x, sy)\) has the even property just by the definition of \(\tau\).

If \((x, sy) = 2(a, sb) \oplus (z, s)\), then by Lemma 2.16 (2), \(\tau(x, sy) = 2\tau(a, sb) \oplus \tau(z, s)\), and it follows that:

\[
(x, sy) = 2(a, sb) \oplus \tau(2(a, sb)) \oplus (z, s) \oplus \tau(z, s)
= (z, s) \oplus [(z, s) \oplus (0, 0)]
= (0, 0)
\]

Then we have \(\tau(x, sy) = (x, sy) \oplus (0, 0) = (x^{-1}, -\frac{sy}{z^2})\), and we obtain that the pair \((x, sy)\) has the odd property just by the definition of \(\tau\).

Lemma 2.21 A function in \(\mathcal{M}\) which is algebraic over \(K(z)\) is a rational function.

Proof: The proof is easy and is left to the reader.

We can now prove the key theorem of this article.

Theorem 2.22 The solutions \((x, y)\) of Equation (MD) over the field \(\mathcal{M}\) of global meromorphic functions are rational.

Proof: Assume that \((x, y)\) is a solution of Equation (MD), \(x\) and \(y\) being functions in \(\mathcal{M}\). By Lemma 2.17, the pair

\[
2(x \circ z^{-1}, -\frac{s}{z^2}y \circ z^{-1}) \in \mathcal{E}(\mathcal{M}^*)
\]

must be equal to \(\pm 2(x, sy)\). We get

\[
x_2 \circ x(z^{-1}) = x_2 \circ x,
\]

which implies by Lemma 2.5 that \(x_2 \circ x\) is a rational function. We conclude by Lemma 2.21 that \(x\) must be rational.

Note that Lemma 2.21 is not necessary for proving Theorem 2.22, because \(x_2\) has constant coefficients. Actually we will need Lemma 2.21 in order to finish the proof of Theorem A.
2.5 Proof of Theorem A

We will prove that Theorems 2.22 and Berkovich’s Theorem, together, give a complete characterization of all the analytic projective maps from $E$ minus a point to $E$.

**Proposition 2.23** Any elliptic curve defined over a field $F$ of characteristic $\neq 2, 3$ is isomorphic (over an algebraic closure $\bar{F}$ of $F$) to the curve with affine equation

\[ y^2 = x^3 + \delta x^2 + x \]

for some $\delta \in \bar{F}$.

**Proof:** Let us write $E_\delta$ the elliptic curve defined by Equation (1). Replacing $x$ by $x - \frac{\delta}{3}$ in Equation (1), we obtain

\[ y^2 = x^3 + (-\frac{\delta^2}{3} + 1)x + (2\frac{\delta^3}{27} - \frac{\delta}{3}) \]

It is then easy to compute the $j$-invariant of the curve $E_\delta$ (see for example [23] for a definition and some basic properties of the $j$- invariant of an elliptic curve). We obtain

\[ j(E_\delta) = 1728 \frac{4(-\delta^2 + 3)^3}{27(4 - \delta^2)} \]

It is clear that the map

\[ j : \bar{K} - \{\pm 2\} \rightarrow \bar{K} \]

\[ \delta \mapsto j(E_\delta) \]

is surjective. \hfill $\diamond$

We denote by $\mathcal{A}(z, w)$ the ring of analytic functions on $K^2$ and by $\mathcal{M}(z, w)$ the field of meromorphic functions on $K^2$, in the variable $(z, w)$. In this section, by $\mathcal{A}(z)$ and $\mathcal{M}(z)$ we denote respectively the ring of global analytic functions and the field of global meromorphic functions of the variable $z$.

Let $E$ be the elliptic curve defined by the affine equation

\[ w^2 = z^3 + \delta z^2 + z. \]

Let $\sim$ denote the equivalence relation on $\mathcal{A}(z, w)$ and $\mathcal{M}(z, w)$ defined by: $f(z, w) \sim g(z, w)$ if and only if, for all $(z, w) \in K^2$, whenever $w^2 = z^3 + \delta z^2 + z$, we have $f(z, w) = g(z, w)$. Let $\mathcal{A}(E) = \mathcal{A}(z, w)/\sim$ and $\mathcal{M}(E) = \mathcal{M}(z, w)/\sim$. An element of $\mathcal{A}(E)$ is called an analytic function on $E$ and an element of $\mathcal{M}(E)$ is called a meromorphic function on $E$. Let $s$ be an element in an algebraic closure of $\mathcal{M}(z)$ satisfying

\[ s^2 = z^3 + \delta z^2 + z. \]

It is trivial to see that

- The polynomial $w^2 = z^3 + \delta z^2 + z$ is irreducible over $\mathcal{M}(z)$. Hence $s$ is an element of degree 2 over $\mathcal{M}(z)$ and integral over $\mathcal{A}(z)$.

- We may identify $\mathcal{A}(E)$ with the ring $\mathcal{A}(z)[s]$ and $\mathcal{M}(E)$ with the field $\mathcal{M}(z)[s]$. 

19
Definition 2.24 A map $G$ from $\mathcal{E} - \infty$ into the projective curve $\mathcal{E}$ is called analytic projective if there exist functions $g_1, g_2, g_3$ in $\mathcal{A}(\mathcal{E})$, not all identically zero, such that

$$(1') \quad g_2^2 g_3 = g_1^3 + \delta g_1^2 g_3 + g_1 g_3^3.$$ 

Note that the relation $(1')$ is obtained by homogenizing Equation (1).

Let $P \in \mathcal{E}$ and $(z_P, s_P) = (z, s) \oplus P$. We will say that $G$ is an analytic projective map on $\mathcal{E} - P$ and into $\mathcal{E}$ if $G$, as a function of $(z_P, s_P)$, is an analytic projective map from $\mathcal{E} - \infty$ into $\mathcal{E}$. If $G$ is not the constant $(0, 0, 1)$, we will represent it by the pair $\left( \frac{a}{g_3}, \frac{b}{g_2} \right)$.

Let $G = (u, v)$ be an analytic projective map on $\mathcal{E} - \infty$ into $\mathcal{E}$. It is obvious from the remark above that $u$ and $v$ can be written as $u = u_0 + su_1$ and $v = v_0 + sv_1$ with $u_i$ and $v_i$ in $\mathcal{M}(z)$. We will say that $G$ is rational if the functions $u_i$ and $v_i$, for $i = 0, 1$, are rational functions (they lie in $K(z)$).

**Proof of Theorem A:**

Without loss of generality, we will work with $P = \infty$. Let $G$ be an analytic projective map on $\mathcal{E} - \{ \infty \}$ into $\mathcal{E}$. Define

$$G^+(z, s) = G(z, s) \oplus G(z, -s)$$
$$G^-(z, s) = G(z, s) \ominus G(z, -s)$$

Assume that $G^+$ and $G^-$ are not $\infty$. Write $G^+ = (a^+, b^+)$ and $G^- = (a^-, b^-)$. It is clear from the addition formula that $a^+, b^+, a^-$ and $b^-$ lie in $\mathcal{M}(\mathcal{E})$, and that the maps $G^+ = (a^+, b^+) \ominus G^- = (a^-, b^-)$ can be written as $G^+ = (a_0^+, sa_1^+, b_0^+, sb_1^+)$ and $G^- = (a_0^-, sa_1^-, b_0^-, sb_1^-)$. Moreover we have:

$$G^+(z, -s) = G^+(z, s)$$
$$G^-(z, -s) = G^-(z, s)$$

which implies that:

- If $G^+$ is not $\infty$, then $a_i^+ = b_i^+ = 0$, that is, we have $G^+ = (a_0^+, b_0^+)$ and then $G^+$ depends only on $z$.
- If $G^-$ is not $\infty$, then $a_i^- = b_i^- = 0$, that is, $G^- = (a_0^-, sb_i^-)$.

By Berkovich’s Theorem, $G^+$ is a constant. Moreover, the coordinates of $G^-$ satisfy

$$ \left( sb_i^- \right)^2 = (a_0^-)^3 + \delta (a_0^-)^2 + a_0^-$$

and then we have

$$ (z^3 + \delta z^2 + z)(b_i^-)^2 = (a_0^-)^3 + \delta (a_0^-)^2 + a_0^-$$

Therefore, $(a_0^-, b_i^-)$ is a solution of Equation (MD) over $\mathcal{M}$. By Theorem 2.22, $G^-$ is rational. Observe that

$$G^+(z, s) \oplus G^-(z, s) = 2G(z, s)$$

It follows that $2G$ is rational. Write $2G = (a, b)$ and $G = (u, v)$ so that

$$\frac{(a^2 - 1)^2}{4F(u)} = a \in K(z, s)$$
Observe that $K(z, s)$ is an algebraic extension of degree 2 of $K(z)$ and then $u$ is algebraic over $K(z)$. Write $u = u_0 + su_1$ and $\bar{u} = u_0 - su_1$, where $u_0$ and $u_1$ are functions in $\mathcal{M}$. It is clear that $\bar{u}$ is algebraic over $K(z)$, therefore $u + \bar{u} = 2u_0$ and $u - \bar{u} = 2su_1$ are algebraic over $K(z)$. So $u_0$ and $u_1$ are both algebraic over $K(z)$. By Lemma 2.21, $u_0$ and $u_1$ are rational functions. So $u$ is a rational function. By similar arguments, it is easy to see that $v$ is also rational. Therefore $G$ is a rational map. The cases in which any of $G^+$ or $G^-$ is the point $\infty$ are similar.

3 Proof of Theorem B

What remains to be proved in order to obtain Theorem B follows by techniques by J. Denef in [8].

Equation (MD)

$$(z^3 + \delta z^2 + z)y^2 = x^3 + \delta x^2 + x$$

defines an elliptic curve $\mathcal{E}^*$ over the field of rational functions $K(z)$, and the point $(z, 1)$ lies on $\mathcal{E}^*$. For any $n$ in the ring $\text{End}(\mathcal{E})$ of endomorphisms of $\mathcal{E}$, let us write

$$(x_n, y_n) = n(z, 1)$$

Note that the addition on $\mathcal{E}^*$ is induced by the addition on $\mathcal{E}$:

$$(x, sy) \in \mathcal{E} \iff (x, y) \in \mathcal{E}^*.$$  

We could define $(x_n, y_n)$ by: $(x_n, sy_n) = n(z, s)$, where the addition is now meant on $\mathcal{E}$. We know by the addition formula that $x_n$ and $y_n$ lie in $K(z)$.

Lemma 3.1 For $n \in \text{End}(\mathcal{E}) - \{0\}$, we have

$$\frac{x_n'}{y_n} = n$$

Proof: See [19, lemma 1.2] or [24, Sect. 8.6].

Corollary 3.2 For $n \in \text{End}(\mathcal{E}) - \{0\}$, the order of $x_n$ at 0 is equal either to 1 or to −1 and $\text{ord}_0(y_n) = \text{ord}_0(x_n) - 1$. Moreover, for $n \in \text{End}(\mathcal{E}) - \{0\}$, we have

$$\frac{x_n}{zy_n}|_{z=0} = \begin{cases} n & \text{if } \text{ord}_0(x_n) > 0 \\ -n & \text{if } \text{ord}_0(x_n) < 0 \end{cases}$$

Proof: From Equation (MD), we see that the order at 0 of $x_n$ cannot be zero (since by the definition, $x_n$ is not constant). By Lemma 3.1 we have

$$\text{ord}_0(y_n) = \text{ord}_0(x_n') = \text{ord}_0(x_n) - 1.$$  

From Equation (MD), equating the order at 0 of both sides, we get

$$1 + 2\text{ord}_0(y_n) = \text{ord}_0(x_n^3 + \delta x_n^2 + x_n) = \begin{cases} \text{ord}_0(x_n) = \text{ord}_0(y_n) + 1 & \text{if } \text{ord}_0(x_n) > 0 \\ 3\text{ord}_0(x_n) = 3(\text{ord}_0(y_n) + 1) & \text{if } \text{ord}_0(x_n) < 0 \end{cases}$$

If $\text{ord}_0(x_n) > 0$, we find $\text{ord}_0(y_n) = 0$ and $\text{ord}_0(x_n) = 1$. While if $\text{ord}_0(x_n) < 0$, we find $\text{ord}_0(y_n) = -2$ and $\text{ord}_0(x_n) = -1$. We conclude by Lemma 3.1. If $\text{ord}_0(x_n) = 1$, we obtain $\frac{x_n}{zy_n}|_{z=0} = n$, and if $\text{ord}_0(x_n) = -1$, we obtain $\frac{x_n}{zy_n}|_{z=0} = -n$. ⊓⊔
Corollary 3.3 For \( n \in \text{End} (\mathcal{E}) - \{0\} \), the order at 0 of \( x_{2n} \) is \(-1\), and the order at 0 of \( x_{2n+1} \) is 1.

Proof: It is clear by the definition that \( \text{ord}_0(x_1) = 1 \). From the duplication formula, we get

\[
x_2(z) = \frac{(z^2 - 1)^2}{4(z^3 + \delta z^2 + z)},
\]

therefore we have \( \text{ord}_0(x_2) = -1 \). On the one hand, we have

\[
x_{2n} = x_2 \circ x_n = \frac{(x_n^2 - 1)^2}{4x_n(x_n^2 + \delta x_n + 1)}.
\]

By Corollary 3.2, we have only two cases: either \( \text{ord}_0(x_n) = 1 \) or \( \text{ord}_0(x_n) = -1 \). In both cases, one can see that \( \text{ord}_0(x_{2n}) = -1 \).

Let us prove by induction that \( \text{ord}_0(x_{2n+1}) = 1 \). The addition formula gives

\[
x_{2n+1} = (z^3 + \delta z^2 + z) \frac{zy_{2n} - x_{2n}}{z x_{2n}(z - x_{2n})^2}.
\]

We write

\[
\frac{zy_{2n} - x_{2n}}{z - x_{2n}} = 1 - \frac{y_{2n}}{z y_{2n}}
\]

Since \( \text{ord}_0(x_{2n}) = -1 \), we have, by Corollary 3.2, \( \text{ord}_0(y_n) = -2 \). We know also by Corollary 3.2 that \( \frac{y_{2n}}{z y_{2n}}|_{z=0} = -n \). Therefore we obtain

\[
\text{ord}_0 \left( \frac{zy_n - x_n}{z - x_n} \right) = 0
\]

which implies that

\[
\text{ord}_0(x_{n+1}) = \text{ord}_0(z^3 + \delta z^2 + z) - \text{ord}_0(z x_n).
\]

It is then clear that \( \text{ord}_0(x_{n+1}) = -\text{ord}_0(x_n) \). \( \diamond \)

For the next theorem, one can refer to [8, part 3], or to [18].

Theorem 3.4 [Denef] Suppose that the elliptic curve \( \mathcal{E} \) has no complex multiplication.

1. All the rational solutions of Equation (MD) are of the form

\[
(x_n, y_n) \oplus (a, b)
\]

where \((a, b)\) is either the neutral or a point of order 2 of \( \mathcal{E}^* \).

2. The set \( \{(x_n, y_n) \mid n \in \text{End}(\mathcal{E})\} \) is existentially definable in the field of rational functions \( K(z) \).
Proof of Theorem B:

Choose an elliptic curve \( E \) such that \( \text{End}(E) = \mathbb{Z} \). Let \( \mu \) be a function in \( \mathcal{M} \). Then \( \mu \in \mathbb{Z} \) if and only if the following formula \( \varphi(\mu) \) (which depends on \( \delta \)) holds:

\[
\mu = 0 \lor \exists x, y, a, b, v, w \left[ F(z)b^2 = F(a) \land (x, y) = 2(a, b) \land y \neq 0 \right. \\
\left. \land vzy = x \land \text{ord}_0(v + 2\mu) > 0 \land w^2 = F(2\mu) \right]
\]

Note that the relation \( (x, y) = 2(a, b) \) can be expressed by an existential (actually, quantifier free) formula, using the addition formula on \( E \).

Let \( \mu \in \mathcal{M} - \{0\} \) be such that the formula \( \varphi(\mu) \) is true in \( \mathcal{M} \). Then there exist \( a, b, x, y \in \mathcal{M} \) such that \( (a, b) \) and \( (x, y) = 2(a, b) \) satisfy Equation (MD). By Theorem 2.22, they must be rational. By Lemma 3.4 and since it is an even solution, \( (x, y) \) is of the form

\[
(x_m, y_m) = m(z, 1) = 2(a, b)
\]

for some non-zero integer \( m \). Since \( (z, 1) \) is not an even solution (see Lemma 2.19), it is clear that the integer \( m \) must be even; say \( m = 2n \). Set \( v \in \mathcal{M} \) such that \( v = \frac{z}{y} \). From Corollaries 3.2 and 3.3, we deduce that \( v(0) = -2n \). Since we have \( \text{ord}_0(v + 2\mu) > 0 \), the function \(-2\mu\) must take the same value as the function \( v \) at 0. Therefore we have \( \mu(0) = n \). Since \( (2\mu, w) \) satisfies Equation (1), we know by Berkovich’s Theorem that the function \( \mu \) must be constant. So we have \( \mu = n \).

Let us prove the converse. Suppose \( \mu = n \) is a non-zero integer. Choose \( x = x_{2n}, y = y_{2n}, a = x_n, b = y_n, v = \frac{x_{2n}}{y_{2n}} \) and \( w \) such that \( w^2 = F(2n) \). Using the properties of \( (x_n, y_n) \), it is easy to see that the formula \( \varphi(\mu) \) is satisfied.

The following corollary was proved in [16].

**Corollary 3.5 (Lipshitz-Pheidas)** The positive existential theory of the ring \( \mathcal{A} \), in the language \( \mathcal{L}_{z} \), is undecidable.

**Proof:** We represent each meromorphic function \( x \) of \( \mathcal{M} \) as the quotient of two analytic functions, \( x = \frac{z}{x_2} \), with \( x_1, x_2 \in \mathcal{A} \) and \( x_2 \neq 0 \); note that, by Berkovich’s Theorem, if \( c \in \mathcal{A} \) then \( c \in K \) if and only if there exists a \( d \in \mathcal{A} \) such that \( c^2 = d^3 + d^2 + d \); and \( c \in K \) is non-zero if and only if there exists \( d \in K \) such that \( cd = 1 \). Also \( \text{ord}_0(x) \) is greater than 0 if and only if the following holds (division is understood in \( \mathcal{A} \)):

“There exists \( c \in K^* \) such that \( z \) divides \( x_2 - c \) and \( z \) divides \( x_1 \).”

It is then obvious that every existential formula of \( \mathcal{L}_z^* \) satisfied in \( \mathcal{M} \) is equivalent to an existential formula satisfied in \( \mathcal{A} \). Finally note that if \( x_2 \in \mathcal{A} \), then \( x_2 \neq 0 \) if and only if there exist \( c, e, f \in K \) such that \( ef = 1 \) and \( z - c \) divides \( x_2 - e \) in \( \mathcal{A} \). Therefore every existential formula of \( \mathcal{L}_z \) satisfied in \( \mathcal{A} \) is equivalent to a positive existential formula of \( \mathcal{L}_z \) satisfied in \( \mathcal{A} \). Hence the result follows. \( \diamond \)

**References**


