UNIVERSITÉ D'ANGERS — Année : 2001

U.F.R. SCIENCES — N° d'ordre : 487

ELEMENTARY EQUIVALENCE OF ELLIPTIC FIELDS

HILBERT'S TENTH PROBLEM FOR p-ADIC GLOBAL MEROMORPHIC FUNCTIONS

Thèse de doctorat

Spécialité : Mathématiques

ÉCOLE DOCTORALE D'ANGERS

Présentée et soutenue publiquement

le 28 septembre 2001
à l'université d'Angers
par Xavier VIDAUX

Devant le jury ci-dessous :

A. Macintyre	Président, Rapporteur	Université d'EDIMBOURGH, Grande Bretagne
A. Pheidas	Examinateur	Université d'HÉRAKLION, Grèce
J. V. Geel	Examinateur	Université de GAND, Belgique
A. Escassut	Examinateur	Université de CLERMONT-FERRAND
L. Lipshitz	Rapporteur	Université de PURDUE, USA

Directeur de thèse : J. - L. Duret Université d'ANGERS

Département de Mathématiques, 2 Bd Lavoisier, 49045 Angers, France ED 363

Merci à Jean-Louis Duret et à Thanasis Pheidas, d'abord pour la confiance qu'ils m'ont toujours accordée, mais aussi pour le temps (et parfois l'argent) qu'ils n'ont pas compté pendant ces quatre années de thèse. Je les remercie aussi pour la grande sagesse qu'ils ont *essayé* de me transmettre tout au long de mon initiation au métier de chercheur (je n'y ai pas été toujours très réceptif, à mon grand dam).

Merci aux membres du jury et en particulier à Leonard Lipshitz et Angus Macintyre pour avoir accepté de rapporter mon travail.

Je tiens aussi à remercier en particulier Alain Escassut pour avoir pris le temps de lire une première version de la thèse et pour toutes les discussions p-adiques (surtout électroniques) qui ont suivi.

Merci aux universités d'Angers et d'Héraklion (en Grèce) et surtout à leur département de mathématiques respectif pour leur soutien matériel, administratif, moral.

Merci en particulier à Luck Darnière, Marie-France Allain, Abdul Darwich, François Lucas, Michel Brestovski, Daniel Schaub, James Alexander, Igor Reider, Jean-Jacques Loeb, Michel Granger, et tout ceux que j'oublie, pour les longues discussions, scientifiques entre autres.

Pardon à Annie Millet et à Renia Pheidas d'avoir parfois accaparé leur mari respectif en dehors des heures légales de travail (mille merci pour leur gentillesse).

Merci à mes parents, pour leur attention tout au long de mes études, pour leur aide financière, mais surtout pour m'avoir encouragé dans des moments de décision critiques; et merci à mon frère et mes soeurs pour avoir su me distraire de mes soucis scientifiques plus d'une fois.

Merci à tous mes amis, de Grèce, d'Angers, de Lyon, de Tahiti, et d'enfance (une pensée amicale pour Hans le marin hollandais et pour Reine Defanti de Châtillon d'Azergues).

Merci à Catherine Gourion pour m'avoir toujours soutenu.

Merci aux mauritaniens Yacoub, Tayeb, Lémine, Limam et sa femme Muriel, et tous les autres qui ont apporté beaucoup de soleil et de rires avec eux lors de leurs années à Angers.

Un pensée particulière pour Alekos et sa famille (le seul periptero francophone d'Héraklion).

Merci à ma grande famille, sur laquelle j'ai toujours pu compter.

Merci à Rania pour avoir supporté mes humeurs lors de cette aventure.

Un grand merci à la Grèce, et à l'organisme grec IKY en particulier, qui m'a permis de terminer ma thèse dans de meilleures conditions que je ne l'avais commencée.

Enfin, merci à tous ceux qui, ne m'ayant pas fait confiance, m'ont obligé à trouver des solutions originales donc enrichissantes.

Contents

1 History - Setting of the problems - Main results

This thesis is dealing with logical properties of fields of functions.

In the first part, we study function fields of curves. Our investigation is motivated by the problem of the decidability (or undecidability) of the theory of the field $\mathbf{C}(z)$ of rational functions. The field $\mathbf{C}(z)$ being a curve field, this question led J.-L. Duret to make the following conjectures :

(C1) *Let K be a curve field over an algebraically closed field k. There exists a subset A of k such that any curve field over k elementarily equivalent to K, in the language of fields augmented by constant symbols for the elements of A, is k-isomorphic to K.*

(C2) *Two curve fields over an algebraically closed field k are elementarily equivalent in the language of fields if and only if they are isomorphic.*

Curves are classified in algebraic geometry up to birational equivalence. These conjectures assert that the classification of curve fields up to elementary equivalence corresponds to the classification of the algebraic geometry.

J.-L. Duret proved both conjectures when K is a curve field of genus $\neq 1$, whatever the characteristic of k is, and, if the characteristic of k is zero, when the field K has genus 1 (such fields are called elliptic fields) and no complex multiplication (see [19]).

The first part contains two articles. We study, in these articles, the conjecture (C1) when k has characteristic zero, and K has genus 1 and complex multiplication :

(CM1) *Let K be a curve field of genus 1, with complex multiplication, over an algebraically closed field k of characteristic zero. There exists a subset A of k such that any curve field over k elementarily equivalent to K, in the language of fields augmented by constant symbols for the elements of A, is k-isomorphic to K.*

We prove, in the second article (see section 4), the following theorem :

Main Theorem 1.1 *Let k be an algebraically closed field of characteristic zero. Let K and K' be two elliptic fields over k. Assume that K has complex multiplication and modular invariant j. Let $\mathcal{L}(j)$ denote the language of fields augmented by a symbol of constant for j. Let E and E' be curves whose function fields are respectively K and K'. If the fields K and K' are elementarily equivalent in the language $\mathcal{L}(j)$, then the curves E and E' have isomorphic rings of endomorphisms.*

This does not prove (CM1), since there exist curves having the same ring of endomorphisms but non k-isomorphic function fields (see Examples 4.20). A theorem analogue to our Main Theorem 1.1 has been obtained by D. A. Pierce in the language of k-algebras (see [37]). We obtain the main theorem 1.1 by combining several techniques and results from [18], [19], [37], and [47] (here in section 3). See section 4.1 for more detailed information on this first part.

The second part of this thesis is dealing with an analogue of Hilbert's tenth problem for p-adic global meromorphic functions. Hilbert's tenth problem, the tenth in the famous list of problems proposed by Hilbert in his 1900's address, is : (translation from German)

(HTP) *Determination of the solvability of a Diophantine equation. Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients : To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

In modern mathematical language, we would ask :

To find an algorithm which decides, for any given Diophantine equation, whether the equation has or does not have integer solutions.

Hilbert's tenth problem was answered negatively by Y. Matiyasevich in 1970 (see section 2 for the basic definitions of logic) :

The positive existential theory of the ring $\mathbf{Z}$ *of rational integers is undecidable.*

It was natural, after this negative answer, to ask the similar question for various other rings and fields. Hilbert's tenth problem for the field $\mathbf{Q}$ of rational numbers is still an open problem. But it is known that the theory of $\mathbf{Q}$ is undecidable (see [43]). The first undecidability results for rings other than the ring of rational integers were obtained by J. Denef and L. Lipshitz (see, for example, [10] or [14]). They obtained undecidability results for various rings of algebraic integers (e.g. : $\mathbf{Z}[i]$). But Hilbert's tenth problem for the ring of algebraic integers in an arbitrary number field is still an open problem.

Let $\mathcal{L}_R$ denote the language of rings, $\mathcal{L}_R^z$ the language of rings augmented by a constant symbol for the variable z, and $\mathcal{L}_R^*$ the language $\mathcal{L}_R^z$ augmented by a symbol for the unary relation $\mathrm{ord}_0(x) > 0$ (that is, the function x takes the value 0 at 0).

Various analogues of Hilbert's tenth problem for polynomial rings over integral domains, in the language $\mathcal{L}_R^z$, have a negative answer (see [11] and [12]). In [11], J. Denef proves that Hilbert's tenth problem for rational function fields over a formally real field K is undecidable in $\mathcal{L}_R^z$. The similar question for $\mathbf{C}(z)$ is still an open problem. Even the whole theory of $\mathbf{C}(z)$ is not known to be decidable or undecidable. More generally, there is no undecidability result for a rational function field $K(z)$, when K is an algebraically closed field of characteristic zero. Several results are known for fields K of positive characteristic (see, for example, [38]). K. Zahidi has obtained undecidability results for various finite algebraic extensions of $\mathbf{R}(z)$ (see [48] or [49]).

For the complex case, R. Robinson proved in [44] that the theory of the ring of analytic functions on a set containing a real open interval is undecidable in the language $\mathcal{L}_R^z$. The analogue in the p-adic case is not known. The existential theory of the ring of functions of two variables, analytic on a subset of $\mathbf{C}^2$ with non-empty interior, is known to be undecidable in $\mathcal{L}_R^z$ (see [40], section 8). The existential theory of the ring of p-adic global analytic functions, in the language $\mathcal{L}_R^z$, was proved to be undecidable in [32]. The main theorem of the second part of this thesis generalizes (and gives a different proof of) this result. No similar result is known for fields of meromorphic functions. In particular, the existential theory of the field of global meromorphic functions on the complex plain is not known to be decidable or undecidable, in any of the languages $\mathcal{L}_R^z$ or $\mathcal{L}_R^*$.

On the other hand, the theory of an arbitrary algebraically closed field, in the language $\mathcal{L}_R$, is decidable (so the existential theory is decidable). In particular, the theory of the field $\mathbf{C}_p$ (the completion of an algebraic closure of the field $\mathbf{Q}_p$ of p-adic numbers) is decidable in $\mathcal{L}_R$. It is easy to see that if the existential theory of a field F is decidable in the language $\mathcal{L}_R$, then the existenial theory of the field $F(z)$ of rational functions over F is decidable in the language $\mathcal{L}_R$ (see [41, Lemma 2.2, p. 12]). As a consequence the existential theory of the field $\mathbf{C}_p(z)$ is decidable in the language $\mathcal{L}_R$. It is a trivial observation that the analogue statements and their proofs, for the field $\mathcal{M}_p$ of p-adic global meromorphic functions, remain correct. Hence, in order to get a non-trivial extension of Hilbert's tenth problem to $\mathbf{C}_p(z)$ and to $\mathcal{M}_p$, we have to extend $\mathcal{L}_R$ by some constant or relation symbol.

The theory of the field $\mathbf{Q}_p$ of p-adic numbers is decidable (see [2] and [23]). An alternative approach to the definability of $\mathbf{Q}_p$ is due to A. Macintyre (see [33]): he proved that the theory of $\mathbf{Q}_p$ in the language $\mathcal{L}_R$, augmented by a predicate P_n for each positive integer n, such that $P_n(x)$ holds if and only if x is an n^{th} power, has elimination of quantifiers (any formula is equivalent to a formula without quantifiers). The same result has been obtained by J. Denef with a purely algebraic proof (see [13]). If the theory of a field K of characteristic zero is decidable, then the theory of the ring $K[[T]]$ of formal power series in one variable over K is decidable (see [27]). F. Delon has proved that the theory of a ring of formal power series in more than one variable is undecidable (see [9]).

The Artin Approximation property allows one, in some cases, to prove decidability results. In particular, the positive existential theory of the ring of germs of complex functions of one variable is decidable. L. van den Dries has obtained results similar to Artin's Approximation, for complex analytic functions on compact sets in [21], and for the p-adic analytic functions on the closed unit disc in [22]. See [41, section 7], for a survey of more related results.

Let $\mathcal{L}_R^T$ denote the language of rings augmented by a symbol $T(x)$ for the unary relation "x is not a constant". The question of the decidability of a rational function field $K(z)$ in the language $\mathcal{L}_R^T$ is related to the following geometric problem:

Let V be an affine variety over the prime field of K. Is there an algorithm to decide whether V contains a curve which admits a $K(z)$-rational parametrization ? (or equivalently, is there a non-constant rational map from the affine line to V ?)

For any field K for which the existential theory of $K(z)$, in the language $\mathcal{L}_R^T$, is decidable, the above geometric problem has a positive answer (but no such K is known); while if the existential theory of $K(z)$, in the language $\mathcal{L}_R^T$, is undecidable, we cannot conclude immediately that the answer to the geometric problem is negative, but a negative answer would be, naturally, more likely than a positive one. L. Rubel, in [45], proves that the positive existential theory of the ring of functions which are analytic on the open complex unit disc, in the language $\mathcal{L}_R^T$, is decidable. No analogue of this result is known for the p-adic case.

There exist examples of structures having their full theory undecidable, whereas their positive existential theory is decidable. Let $\mathcal{L} = \{+, |, 0, 1\}$ denote the language of addition and divisibility. The full theory of N, in the language $\mathcal{L}$, is undecidable (see [43]), while its positive existential theory is decidable (see [31]). If K is a field with decidable existential theory, then the polynomial ring in one variable $K[T]$ gives another example of such a structure.

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

$$P_i(f_1, \cdots, f_k) = 0, \quad \mathrm{ord}_0(f_j) > 0, \qquad i = 1, \cdots, n \quad \text{and} \quad j = 1, \cdots, k$$

where P_i, for $i = 1, \cdots, n$, are polynomials with coefficients in $\mathbf{Z}(z)$, and the variables $f_1, \ldots, f_k$ range in $\mathcal{M}_p$. One may consider that we deal with systems of differential equations "of order zero", together with initial conditions ($\mathrm{ord}_0(f_j) > 0$). From this point of view, the language $\mathcal{L}_R^*$ 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 $\mathcal{L}_R^z$. However, the problem of defining existentially the relation $\mathrm{ord}_0(f) > 0$ in the language $\mathcal{L}_R^z$ over a field of functions is in general not trivial. In particular the problem is open for $\mathbf{C}(z)$ as well as for the field of complex meromorphic functions (see [41, §2.5]).

Here is a summary of our results of the second part :

Main Theorem 1.2 1. *The set of rational integers is positive existentially definable in the field $\mathcal{M}_p$ of p-adic global meromorphic functions in the language $\mathcal{L}_R^*$.*

2. *The positive existential theory of $\mathcal{M}_p$ in the language $\mathcal{L}_R^*$ is undecidable.*

A consequence of our result is the similar result for global analytic functions, in the language $\mathcal{L}_R^z$, which was proved before, in [32]. In order to prove the main theorem 1.2, we obtain the following intermediate results :

1. *We obtain a characterization of the p-adic meromorphic parametrizations of an elliptic curve, defined over the field of constants, extending a result of W. Berkovich (see section 7). See [4, chap. 4, thm. 4.5.1], or [5, cor. a, p. 3], for alternative proofs of Theorem 7.1.*

2. *We obtain a complete characterization of all p-adic analytic projective maps from an elliptic curve $\mathcal{E}$, minus a point, to the elliptic curve $\mathcal{E}$ (for any elliptic curve defined over the field of constants). See subsection 8.5.*

Some obvious open problems, related to our results of the second part of this thesis, are :

Question 1 : Is the analogue of the main theorem 1.2 true in the complex case ?
Q. 2 : Is the analogue of the main theorem 1.2 true in the language $\mathcal{L}_R^z$?
Q. 3 : Is the analogue of the main theorem 1.2 true in the language $\mathcal{L}_R^T$?
Q. 4 : Is the relation "$ord_0(x) > 0$" definable in the ring theory of $\mathcal{M}_p$? Existentially definable ?

Q. 5 : Let $D = D(0, r)$ be the disk of $\mathbf{C}_p$ of center 0 and radius r, with or without boundary. Let $\mathcal{M}_p(D)$ be the field of meromorphic functions on D (see section 6.5 for a precise definition). Is the theory of $\mathcal{M}_p(D)$, in the language $\mathcal{L}_R^*$, decidable ? And what about the existential theory ?

In our effort to prove the main theorem 1.2 of the second part, we had to develop tools and methods in p-adic analysis which seemed not to exist in the bibliography. After having done so, we were informed that some of our intermediate results were known before, by methods of rigid analysis and p-adic Nevanlinna's theory. Such results will be indicated in the text of the relevant sections.

2 Basic definitions and notation of mathematical logic

This section contains most of the vocabulary we use from mathematical logic, presented in a rather informal way. Precise definitions may be found in any basic book of mathematical logic (e.g. :[6], [7]).

For our purpose, a *language* $\mathcal{L}$ is defined by a set $\{A, B, C\}$, where :

- $A =$ the set of logical symbols : $\forall$ (universal quantifier), $\exists$ (existential quantifier), $\neg$ (negation), $\vee$ (or), and $\wedge$ (and);
- $B =$ an infinite set of symbols for variables;
- $C =$ a set of symbols for functions (including constant symbols), and symbols for relations.

To describe a language, it suffices to give the elements of the set C. We will always consider *finite languages* (e.g. : C is finite), with a symbol for equality "=". For example, the *language of rings* is the set $\mathcal{L}_R = \{0, 1, +, .\}$, where 0 and 1 are constant symbols and $+$, . are symbols for functions of two variables.

A *formula* of a language $\mathcal{L}$ is built from the elements of $\mathcal{L}$ in the usual way. A *sentence* is a formula without *free variables* (all variables are in the scope of some quantifier). In the language of rings, any formula is equivalent to one with a finite set of quantifiers followed by a boolean combination of polynomial equations and inequations with rational integer coefficients. A *sentence interpreted in a structure* is either *true* or *false.* Let us give an example. The sentence $\forall x \exists y (y^2 = x)$ is true in $\mathbf{R}$ but is false in $\mathbf{Q}$. An *existential* formula is a formula which is equivalent to one of the form $\exists x \phi(x)$, $x = x_1, \dots, x_n$, where ϕ contains no quantifier. We say that the formula is *positive existential* if moreover ϕ contains no negation symbol.

The *theory* (resp. *existential theory, positive existential theory*) of a structure is the set of sentences (resp. existential sentences, positive existential sentences) which are true in this structure. A set of sentences S is *decidable* if there is an algorithm to decide whether or not a sentence belongs to S. A set of sentences which is not decidable is said to be *undecidable.* It is clear that if the positive existential theory of a structure is undecidable, then the existential theory as well as the theory of this structure is undecidable.

A subset S of a structure M is *definable* (resp. *existentially definable, positive existentially definable*) in M, for a language $\mathcal{L}$, if there exists a formula (resp. an existential formula, a positive existential formula) $\varphi(x)$, in the language $\mathcal{L}$, which is true in M if and only if x belongs to S.

In the following, $\mathcal{L}_R$ will denote the language of rings, $\mathcal{L}_R^z$ the language of rings augmented by a constant symbol for the variable z, and $\mathcal{L}_R^*$ the language $\mathcal{L}_R^z$ augmented by a symbol for the unary relation $\mathrm{ord}_0(x) > 0$ (that is, the function x takes the value 0 at 0).

Part I
ÉQUIVALENCE ÉLÉMENTAIRE DE CORPS ELLIPTIQUES

3 Équivalence élémentaire de corps elliptiques - A

C. R. Acad. Sci. Paris, t. 330, Série I, p. 1-4, 2000
Logique/*logic*

ÉQUIVALENCE ÉLÉMENTAIRE DE CORPS ELLIPTIQUES

Résumé. Il s'agit de démontrer une partie de la conjecture suivante : deux corps elliptiques sur un corps algébriquement clos k sont k-isomorphes si et seulement s'ils sont élémentairement équivalents dans le langage des corps enrichi d'une constante (l'invariant modulaire). C'est une extension des résultats de Duret sur l'équivalence élémentaire des corps de fonctions.

Elementary equivalence of elliptic fields

Abstract. We prove some part of the following conjecture : two elliptic fields over an algebraically closed field k are k-isomorphic if and only if they are elementarily equivalent in the language of fields expanded with a symbol of constant (the modular invariant). This is an extension of Duret's results about elementary equivalence of function fields.

Si ω_1 et ω_2 sont des nombres complexes $\mathbf{R}$-linéairement indépendants, notons $\langle\omega_1, \omega_2\rangle$ le réseau de $\mathbf{C}$ ayant pour base (ω_1, ω_2). Soit τ un nombre complexe algébrique quadratique. Soit $AX^2 + BX + C$ un polynôme dont il est la racine, avec A un entier naturel strictement supérieur à 0, B et C des entiers relatifs vérifiant $A \wedge B \wedge C = 1$ ($a \wedge b$ désignant le pgcd positif de a et de b). Pour tout entier $n \in \mathbf{N}$ non nul, notons Λ_n le réseau $\langle\frac{1}{n}, \tau\rangle$, E_n le quotient $\frac{\mathbf{C}}{\Lambda_n}$, $\mathrm{Hom}\,(E_1, E_n)$ le sous-groupe de $\mathbf{C}$ $\{\alpha \in \mathbf{C} \mid \alpha\Lambda_1 \subset \Lambda_n\}$, $\mathrm{End}\,(E_1)$ l'anneau $\mathrm{Hom}\,(E_1, E_1)$ et δ_n l'entier $A \wedge nB \wedge nC = A \wedge n$. On a, pour tout entier naturel n strictement positif, $\mathrm{End}\, E_1 \subset \mathrm{Hom}\,(E_1, E_n)$ et si p est un diviseur de n, alors $\mathrm{Hom}\,(E_1, E_p)$ est inclus dans $\mathrm{Hom}\,(E_1, E_n)$.

Proposition 3.1 .
Pour tout entier $n \geq 1$, on a : $\mathrm{Hom}\,(E_1, E_n) = \langle 1, \frac{A}{\delta_n}\bar{\tau}\rangle$.

Démonstration : Pour la première inclusion, on a :

$$\langle 1, \frac{A}{\delta_n}\bar{\tau}\rangle\langle 1, \tau\rangle = \langle 1, \tau, \frac{A}{\delta_n}\bar{\tau}, \frac{A}{\delta_n}\bar{\tau}\tau\rangle = \langle 1, \tau, \frac{-B - A\tau}{\delta_n}, \frac{C}{\delta_n}\rangle = \langle 1, \tau, \frac{B}{\delta_n}, \frac{C}{\delta_n}\rangle \subset \langle\frac{1}{n}, \tau\rangle.$$

Il s'ensuit que le réseau $\langle 1, \frac{A}{\delta_n}\bar{\tau}\rangle$ est inclus dans $\mathrm{Hom}\,(C_1, C_n)$.

Nous montrons l'inclusion réciproque en utilisant un argument analogue à [28, thm. 2, p. 90]. On constate que :

$$\langle\frac{nA}{\delta_n}, \frac{nA}{\delta_n}\bar{\tau}\rangle\langle 1, \tau\rangle = \frac{n}{\delta_n}\langle A, A\bar{\tau}, A\tau, A\tau\bar{\tau}\rangle = \frac{n}{\delta_n}\langle A, -B - A\tau, A\tau, C\rangle = \frac{n}{\delta_n}\langle A, B, A\tau, C\rangle.$$

Or $A \wedge B \wedge C$ est égal à 1, donc 1 est élément de $\langle \frac{nA}{\delta_n}, \frac{nA}{\delta_n}\bar{\tau}\rangle\langle 1, \tau\rangle$. On constate aussi que :

$$\langle \frac{nA}{\delta_n}, \frac{nA}{\delta_n}\bar{\tau}\rangle\langle \frac{1}{n}, \tau\rangle = \frac{1}{\delta_n}\langle A, nA\tau, A\bar{\tau}, nA\tau\bar{\tau}\rangle =$$

$$\frac{1}{\delta_n}\langle A, n(-B - A\bar{\tau}), A\bar{\tau}, nC\rangle = \frac{1}{\delta_n}\langle A, nB, A\bar{\tau}, nC\rangle \subset \frac{1}{\delta_n}\langle \delta_n, A\bar{\tau}\rangle$$

car $A \wedge nB \wedge nC$ est par définition égal à δ_n. Donc on a $\langle \frac{nA}{\delta_n}, \frac{nA}{\delta_n}\bar{\tau}\rangle\langle \frac{1}{n}, \tau\rangle \subset \langle 1, \frac{A}{\delta_n}\bar{\tau}\rangle$. Par conséquent, si nous notons Λ le réseau $\langle \frac{nA}{\delta_n}, \frac{nA}{\delta_n}\bar{\tau}\rangle$, les remarques précédentes se traduisent par : $1 \in \Lambda\Lambda_1$ et $\Lambda\Lambda_n \subset \langle 1, \frac{A}{\delta_n}\bar{\tau}\rangle$. Soit α un élément de $\mathrm{Hom}\,(E_1, E_n)$. On a $\alpha\Lambda_1 \subset \Lambda_n$, donc on a aussi $\alpha\Lambda\Lambda_1 \subset \Lambda\Lambda_n$, mais comme $1 \in \Lambda\Lambda_1$, on a $\alpha \in \Lambda\Lambda_n \subset \langle 1, \frac{A}{\delta_n}\bar{\tau}\rangle$. D'où l'autre inclusion. □

Lemme 3.2 . *Le réseau* $\mathrm{Hom}\,(E_1, E_n)$ *est inclus dans* $\mathrm{Hom}\,(E_1, E_p)$ *si et seulement si* δ_n *divise* p.

Démonstration :

$$\mathrm{Hom}\,(E_1, E_n) \subset \mathrm{Hom}\,(E_1, E_p) \Longleftrightarrow \langle 1, \frac{A}{\delta_n}\bar{\tau}\rangle \subset \langle 1, \frac{A}{\delta_p}\bar{\tau}\rangle \Longleftrightarrow \exists l \in \mathbf{Z}, \frac{A}{\delta_n}\bar{\tau} = \frac{lA}{\delta_p}\bar{\tau}$$

$$\Longleftrightarrow \exists l \in \mathbf{Z}, \delta_p = l\delta_n \Longleftrightarrow A \wedge n \text{ divise } A \wedge p \Longleftrightarrow A \wedge n \text{ divise } p.$$

□

Corollaire 3.3 . *Pour tout entier* $n \in \mathbf{N}^*$, *on a :* $\mathrm{Hom}\,(E_1, E_n) = \mathrm{Hom}\,(E_1, E_{\delta_n})$. *Le plus petit entier naturel* p *tel que* $\mathrm{Hom}\,(E_1, E_n) = \mathrm{Hom}\,(E_1, E_p)$ *est* $p = \delta_n$.

Corollaire 3.4 . *Si* p *et* q *divisent* A, *alors on a l'équivalence suivante :*

$$\mathrm{Hom}\,(E_1, E_p) = \mathrm{Hom}\,(E_1, E_q) \Longleftrightarrow p = q.$$

Corollaire 3.5 . *L'application*

$$\begin{array}{rcl} \{p \in \mathbf{N}^* \mid p \text{ divise } A\} & \longrightarrow & \{\mathrm{Hom}\,(E_1, E_p) \mid p \in \mathbf{N}^*\} \\ p & \longmapsto & \mathrm{Hom}\,(E_1, E_p) \end{array}$$

est une bijection. En particulier, la cardinal de l'ensemble $\{\mathrm{Hom}\,(E_1, E_p) \mid p \in \mathbf{N}^*\}$ *est le nombre de diviseurs de* A.

Démonstration : C'est une application injective par 3.4. Elle est surjective par 3.3. □

Faisons apparaître provisoirement le nombre τ dans les notations. Ainsi notons Λ_n^τ le réseau $\langle \frac{1}{n}, \tau\rangle$, $\mathcal{P}_n^\tau$ la fonction de Weierstrass de Λ_n^τ et $g_2^n(\tau)$ et $g_3^n(\tau)$ les nombres complexes tels que $(\mathcal{P}_n^{\tau\prime})^2 = 4\mathcal{P}_n^{\tau 3} - g_2^n(\tau)\mathcal{P}_n^\tau - g_3^n(\tau)$. Notons $R_n^\tau(X, Y)$ le polynôme $Y^2 - 4X^3 + g_2^n(\tau)X + g_3^n(\tau) \in \mathbf{C}[X, Y]$. Si k est un corps, notons $cl.a.(k)$ sa clôture algébrique. Nous rappelons que (voir [26, pp. 316-336]) pour tout corps de courbe K sur un corps algébriquement clos k, sous-corps de $\mathbf{C}$, d'invariant modulaire j, il existe u et v dans K et des éléments a et b de k tels que $v^2 = 4u^3 - au - b$. Mais j est égal à $1728\frac{a^3}{a^3 - 27b^2}$ donc j est élément de k. Il s'ensuit que k contient $cl.a.(\mathbf{Q}(j))$. Notons j_τ l'invariant modulaire de la courbe elliptique associée à $E_1^\tau = \frac{\mathbf{C}}{\Lambda_1^\tau}$, et Δ_τ le corps $cl.a.(\mathbf{Q}(j_\tau))$. On a l'égalité $cl.a.(\mathbf{Q}(j_\tau)) = cl.a.(\mathbf{Q}(g_2^1(\tau), g_3^1(\tau)))$. D'après [19, prop. 31, p. 816], $g_2^n(\tau)$ et $g_3^n(\tau)$ sont algébriques sur $\mathbf{Q}(g_2^1(\tau), g_3^1(\tau))$, donc ils sont dans Δ_τ. Nous noterons $\mathcal{E}(\Lambda_n^\tau)$ le corps des fonctions méromorphes ayant pour ensemble de périodes Λ_n^τ. On a $\mathcal{E}(\Lambda_n^\tau) = \mathbf{C}(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau\prime})$. Enfin, nous noterons $\mathcal{L}$ le langage des corps et $\mathcal{L}(j_\tau)$ le langage des corps ayant j_τ comme symbole de constante supplémentaire.

Le lecteur remarquera que l'invariant j_τ, et donc aussi Δ_τ, ne dépendent pas de l'entier n. La proposition suivante va nous permettre, en particulier, d'alléger les notations. Nous ne ferons plus varier alors que cet entier n. Si k est un sous-corps de $\mathbf{C}$ algébriquement clos contenant Δ_τ, τ un nombre complexe algébrique quadratique et n un entier naturel strictement supérieur à 1, soit $\mathbf{P}_n^\tau(k)$ la propriété : $\ll k(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau\prime})$ et $k(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau\prime})$ ne sont pas élémentairement équivalents dans le langage $\mathcal{L}(j_\tau) \gg$. Si K est un corps de courbe de genre 1 sur un corps algébriquement clos k de caractéristique 0, avec multiplication complexe et d'invariant modulaire j, et K' un corps de courbe sur k non isomorphe à K, soit $\mathbf{P}_k(K, K')$ la propriété : $\ll K$ et K' ne sont pas élémentairement équivalents dans le langage $\mathcal{L}(j) \gg$.

Proposition 3.6 . *Si la propriété $\mathbf{P}_n^\tau(k)$ est vraie pour tout triplet (k, τ, n), alors la propriété $\mathbf{P}_k(K, K')$ est vraie pour tout couple (K, K').*

Démonstration : On trouve tous les arguments dans la première partie de la démonstration de [19, thm. 35, p. 818]. L'auteur démontre d'abord l'équivalence entre les trois propriétés suivantes ($2 \Rightarrow 1$ puis $3 \Rightarrow 2$) :

1. La propriété $\mathbf{P}_k(K, K')$ est vraie pour tout triplet (k, K, K').

2. La propriété $\mathbf{P}_k(K, K')$ est vraie pour tout triplet (k, K, K') avec k sous-corps de $\mathbf{C}$.

3. La propriété $\mathbf{P}_k(K, K')$ est vraie pour tout triplet (k, K, K') avec K' sous-corps de K et k sous-corps de $\mathbf{C}$.

Si k est un sous-corps de $\mathbf{C}$, alors on a $K \underset{k}{\otimes} \mathbf{C} = \mathcal{E}(\Lambda)$ et $K' \underset{k}{\otimes} \mathbf{C} = \mathcal{E}(\Lambda')$ pour des réseaux Λ et Λ' de $\mathbf{C}$; et comme K' est un sous-corps de K, on a $\Lambda \subset \Lambda'$. D'après [20, §63, p. 132], il existe une base (ω_1, ω_2) de Λ et des entiers naturels non nuls m et n tels que $(\frac{\omega_1}{mn}, \frac{\omega_2}{m})$ soit une base de Λ'. Notons τ le quotient $\frac{\omega_2}{\omega_1}$. Comme $\langle \frac{\omega_1}{mn}, \frac{\omega_2}{m} \rangle$ est similaire à $\langle \frac{\omega_1}{n}, \omega_2 \rangle$, et donc à $\langle \frac{1}{n}, \tau \rangle$, et $\langle \omega_1, \omega_2 \rangle$ est similaire à $\langle 1, \tau \rangle$, $\mathcal{E}(\Lambda)$ et $\mathcal{E}(\Lambda')$ sont $\mathbf{C}$-isomorphes respectivement à $\mathcal{E}(\langle 1, \tau \rangle)$ et à $\mathcal{E}(\langle \frac{1}{n}, \tau \rangle)$. Si nous notons $\mathcal{P}_n^\tau$ la fonction de Weierstrass de $\langle \frac{1}{n}, \tau \rangle$ et $\mathcal{P}_1^\tau$ celle de $\langle 1, \tau \rangle$, $k(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau\prime})$ et $k(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau\prime})$ sont k-isomorphes respectivement à K' et à K. Donc la propriété $\mathbf{P}_k(K, K')$ est équivalente à la propriété $\mathbf{P}(k(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau\prime}), k(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau\prime}))$, ie : $\mathbf{P}_n^\tau(k)$. □

Dorénavant, le corps k et le nombre τ sont fixés, il n'est donc plus nécessaire de les faire apparaître dans les notations.

Lemme 3.7 . *Soit n un entier strictement positif et p un diviseur de n. On a alors $\Lambda_p \subset \Lambda_n$. Soit k un sous-corps de $\mathbf{C}$, extension de Δ.*

1. *Les corps $\Delta(\mathcal{P}_n, {\mathcal{P}_n}')$ et $k(\mathcal{P}_n, {\mathcal{P}_n}')$ sont sous-corps respectivement de $\Delta(\mathcal{P}_p, {\mathcal{P}_p}')$ et de $k(\mathcal{P}_p, {\mathcal{P}_p}')$.*

2. *La fonction de Weierstrass $\mathcal{P}_p$ est élément primitif de $\Delta(\mathcal{P}_p, {\mathcal{P}_p}')$ sur $\Delta(\mathcal{P}_n, {\mathcal{P}_n}')$, de $k(\mathcal{P}_p, {\mathcal{P}_p}')$ sur $k(\mathcal{P}_n, {\mathcal{P}_n}')$ et de $\mathbf{C}(\mathcal{P}_p, {\mathcal{P}_p}')$ sur $\mathbf{C}(\mathcal{P}_n, {\mathcal{P}_n}')$.*

3. *Tout polynôme minimal de $\mathcal{P}_p$ sur $\Delta(\mathcal{P}_n, {\mathcal{P}_n}')$ est polynôme minimal de $\mathcal{P}_p$ sur $k(\mathcal{P}_n, {\mathcal{P}_n}')$ et sur $\mathbf{C}(\mathcal{P}_n, {\mathcal{P}_n}')$. Il existe donc un polynôme $P_p(X, Y, Z)$ à coefficients dans Δ, tel que $P_p(\mathcal{P}_n, {\mathcal{P}_n}', Z)$ soit polynôme minimal de $\mathcal{P}_p$ sur $k(\mathcal{P}_n, {\mathcal{P}_n}')$ et sur $\mathbf{C}(\mathcal{P}_n, {\mathcal{P}_n}')$.*

Démonstration : On applique [19, prop. 32, p. 817] aux réseaux $\Lambda_p \subset \Lambda_n$ en constatant qu'en notant $\omega_1 = \frac{1}{p}$, $\omega_2 = \tau$ et $m = \frac{n}{p}$, on a : $\Lambda_p = \langle \omega_1, \omega_2 \rangle \subset \langle \frac{\omega_1}{m}, \omega_2 \rangle = \Lambda_n$. □

Proposition 3.8 .[Duret] *Pour tout entier n, si* $\operatorname{Hom}(E_1, E_n)$ *est égal à* $\operatorname{End} E_1$*, alors la propriété* $\mathbf{P}_n$ *est vraie.*

Démonstration : Voir la remarque [19, rem. 37, p. 821] relative à [19, thm. 35, p. 818]. □

Théorème 3.9 . *Pour tout entier n, s'il existe un entier p tel que* $1 \leq p < n$ *et* $\operatorname{Hom}(E_1, E_n)$ *est égal à* $\operatorname{Hom}(E_1, E_p)$*, alors la propriété* $\mathbf{P}_n$ *est vraie.*

Démonstration : D'après la proposition 3.8, il suffit de le démontrer si p est strictement supérieur à 1, et d'après le corollaire 3.3, nous pouvons alors choisir $p = n \wedge A$. Soit C une formule définissant k dans $k(\mathcal{P}_n, \mathcal{P}_n')$ et dans $k(\mathcal{P}_1, \mathcal{P}_1')$, et $\mathbf{C}$ dans $\mathbf{C}(\mathcal{P}_n, \mathcal{P}_n')$ et dans $\mathbf{C}(\mathcal{P}_1, \mathcal{P}_1')$ (voir [18, prop. 10, p. 950]). D'après [19, prop. 33, p. 818], il suffit de trouver une formule à coefficients dans Δ. Soit Θ_n la formule

$$\exists x, y \Big(\neg C(x) \wedge R_n(x, y) = 0 \wedge \forall z \; P_p(x, y, z) \neq 0 \Big)$$

où $P_p(X, Y, Z) \in \Delta[X, Y, Z]$ est le polynôme défini dans le lemme 3.7(3).

Il est clair que $k(\mathcal{P}_n, \mathcal{P}_n')$ satisfait la formule Θ_n. Il suffit de choisir $x = \mathcal{P}_n$, $y = \mathcal{P}_n'$ et de conclure d'après le lemme 3.7(3).

Montrons que $k(\mathcal{P}_1, \mathcal{P}_1')$ satisfait la formule $\neg\Theta_n$. Soit donc u et v des éléments de $k(\mathcal{P}_1, \mathcal{P}_1')$ tels qu'on ait : $u \notin k$ et $R_n(u, v) = 0$. Nous cherchons $w \in k(\mathcal{P}_1, \mathcal{P}_1')$ vérifiant $P_p(u, v, w) = 0$. S'il existe un tel w, il est algébrique sur $\Delta(u, v) \subset k(\mathcal{P}_1, \mathcal{P}_1')$. Mais $k(\mathcal{P}_1, \mathcal{P}_1')$ est algébriquement clos dans $\mathbf{C}(\mathcal{P}_1, \mathcal{P}_1')$, donc il existe un tel w dans $k(\mathcal{P}_1, \mathcal{P}_1')$ si et seulement s'il en existe un dans $\mathbf{C}(\mathcal{P}_1, \mathcal{P}_1')$. Les conditions sur u et v donnent un $\mathbf{C}$-isomorphisme de corps :

$$\phi_0 \colon \mathbf{C}(\mathcal{P}_n, \mathcal{P}_n') \xrightarrow{\sim} \mathbf{C}(u, v)$$

où $\phi_0(\mathcal{P}_n) = u$ et $\phi_0(\mathcal{P}_n') = v$. Or on a $\mathbf{C}(\mathcal{P}_n, \mathcal{P}_n') = \mathcal{E}(\Lambda_n)$, donc il existe un nombre complexe non nul α tel qu'on ait $\mathbf{C}(u, v) = \mathcal{E}(\alpha\Lambda_n)$ (voir [20, §90, pp. 195-196]). Mais $\mathbf{C}(u, v) \subset \mathbf{C}(\mathcal{P}_1, \mathcal{P}_1')$, donc on a $\mathcal{E}(\alpha\Lambda_n) \subset \mathcal{E}(\Lambda_1)$, ou en termes de réseaux, $\Lambda_1 \subset \alpha\Lambda_n$, c'est à dire : $\alpha^{-1} \in \operatorname{Hom}(E_1, E_n)$. Donc, et d'après l'hypothèse du théorème, α^{-1} est élément de $\operatorname{Hom}(E_1, E_p)$, ce qui implique que Λ_1 est inclus dans $\alpha\Lambda_p$, ou, en termes de corps, $\mathcal{E}(\alpha\Lambda_p)$ est inclus dans $\mathcal{E}(\Lambda_1)$. Il s'ensuit que nous pouvons étendre ϕ_0 à un $\mathbf{C}$-morphisme de corps :

$$\phi \colon \mathcal{E}(\Lambda_p) \xrightarrow{\sim} \mathcal{E}(\alpha\Lambda_p) \subset \mathcal{E}(\Lambda_1).$$

Choisissons $w = \phi(\mathcal{P}_p)$. On a bien $P_p(u, v, w) = \phi(P_p(\mathcal{P}_n, \mathcal{P}_n', \mathcal{P}_p)) = 0$. □

D'après le corollaire 3.5, il existe p tel que $1 \leq p < n$ et $\operatorname{Hom}(E_1, E_n) = \operatorname{Hom}(E_1, E_p)$ si et seulement si n ne divise pas A. Pour chaque τ donc, et pour chaque k, il reste à trouver la formule Θ_n pour tous les diviseurs n de l'entier A.

4 Équivalence élémentaire de corps elliptiques - B

(accepté pour publication au J. of Symb. Logic*)*

MULTIPLICATION COMPLEXE ET ÉQUIVALENCE ÉLÉMENTAIRE DANS LE LANGAGE DES CORPS

Résumé. Soit K et K' deux corps elliptiques avec multiplication complexe sur un corps algébriquement clos k de caractéristique 0, non k-isomorphes, et soit C et C' deux courbes ayant pour corps de fonctions K et K' respectivement. Nous démontrons que si les anneaux d'endomorphismes de C et de C' ne sont pas isomorphes, alors K et K' ne sont pas élémentairement équivalents dans le langage des corps enrichi d'une seule constante (l'invariant modulaire). Ce travail fait suite à un travail de David A. Pierce qui se place dans le langage des k-algèbres.

-Classification AMS : 03C

Complex multiplication and elementary equivalence in the language of fields

Abstract. Let K and K' be two elliptic fields with complex multiplication over an algebraically closed field k of characteristic 0, non k-isomorphic, and let C and C' be two curves with respectively K and K' as function fields. We prove that if the endomorphism rings of the curves are not isomorphic then K and K' are not elementarily equivalent in the language of fields expanded with a constant symbol (the modular invariant). This theorem is an analogue of a theorem from David A. Pierce in the language of k-algebras.

4.1 Contexte et notations

Nous considérons un corps algébriquement clos k. Un *corps de courbe sur* k est une extension finiment engendrée de degré de transcendance 1 sur k. Pour tout sous-ensemble A de k, $\mathcal{L}(A)$ désigne le langage des corps enrichi de symboles de constantes pour les éléments de A. Dans [19], Jean-Louis Duret propose les deux conjectures, très liées, suivantes. :

(C1) *Soit K un corps de courbe sur k. Il existe un sous-ensemble fini A de k tel que tout corps de courbe sur k élémentairement équivalent à K dans le langage $\mathcal{L}(A)$ lui est k-isomorphe.*

(C2) *Deux corps de courbe sur k sont élémentairement équivalents dans le langage des corps si et seulement s'ils sont isomorphes.*

Les courbes se classent en géométrie algébrique à équivalence birationnelle près. Les conjectures affirment que la classification des corps de courbes à équivalence élémentaire près correspond à la classification de la géométrie algébrique. On peut rapprocher de ce travail l'article [3], où les auteurs étudient si l'élémentaire équivalence des anneaux de fonctions analytiques sur des domaines entraîne l'isomorphisme de ces domaines.

J.-L. Duret (voir [19]) a prouvé les deux conjectures lorsque K est un corps de courbe de genre différent de 1, quelle que soit la caractéristique de k, et, si la caractéristique de k est 0, lorsque le corps K est de genre 1 et sans multiplication complexe. L'objet de cet article est d'étudier la conjecture (C1) dans le cas où le corps k est de caractéristique 0, et le corps de courbe K est de genre 1 avec multiplication complexe (CM1). La spécificité des corps de courbe qui ont une multiplication complexe fait apparaître de nouvelles difficultés. Nous démontrons le théorème suivant.

Théorème principal. *Soit k un corps algébriquement clos de caractéristique* 0*. Soient K et K' des corps de courbe elliptique sur k, le corps K étant avec multiplication complexe et d'invariant modulaire j. Soit $\mathcal{L}(j)$ le langage des corps enrichi d'un symbole de constante pour j. Soient E et E' des courbes dont les corps de fonctions sont respectivement K et K'. Si les corps K et K' sont élémentairement équivalents dans le langage $\mathcal{L}(j)$, alors les courbes E et E' ont des anneaux d'endomorphismes isomorphes.*

Ce théorème ne démontre pas (CM1), car il existe des courbes ayant le même anneau d'endomorphisme mais des corps de fonctions non isomorphes (voir exemples 4.20). Ce même théorème a été démontré par D. A. Pierce dans le langage des k-algèbres (voir [37]). Pour pouvoir passer du langage des k-algèbres au langage $\mathcal{L}(j)$, et donc prouver ce théorème, nous avons du rendre effective la démonstration de D. A. Pierce. Pour cela, nous utilisons de nombreuses techniques et résultats des articles [18], [19], [37], et à moindre mesure, de la section 3.

Nous avions remarqué, dans la section 3, qu'il suffit de démontrer (CM1) lorsque k est un sous-corps de $\mathbf{C}$, et pour une famille de corps K dépendant de deux paramètres : un entier $n \in \mathbf{N}$ et un nombre complexe algébrique quadratique τ. Ceci nous permet d'utiliser des techniques de la théorie des courbes elliptiques sur le corps des nombres complexes. En particulier, nous utiliserons, sans le rappeler, que la catégorie des courbes elliptiques est équivalente à la catégorie des réseaux (voir [46, chap. VI, thm. 5.3, p. 162]).

Nous nous référons à [26], [28] et [46] pour la théorie des courbes elliptiques.

Si ω_1 et ω_2 sont des nombres complexes $\mathbf{R}$-linéairement indépendants, notons

$$\langle \omega_1, \omega_2 \rangle = \{\lambda\omega_1 + \mu\omega_2 \mid \lambda, \mu \in \mathbf{Z}\}$$

le réseau de $\mathbf{C}$ ayant pour base (ω_1, ω_2). Étant donné un réseau Λ, nous noterons $\mathcal{P}(., \Lambda)$ la fonction de Weierstrass du réseau Λ :

$$\mathcal{P}(z, \Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right].$$

Nous noterons $\mathcal{P}'(., \Lambda)$ la dérivée de $\mathcal{P}(., \Lambda)$ et, pour $i = 2, 3$, $g_i(\Lambda)$ les nombres complexes tels que

$$\mathcal{P}'(., \Lambda)^2 = 4\mathcal{P}(., \Lambda)^3 - g_2(\Lambda)\mathcal{P}(., \Lambda) - g_3(\Lambda).$$

Si τ est un nombre complexe algébrique quadratique et $n \geq 1$ un entier, nous noterons

$$\Lambda_n^\tau = \langle \frac{1}{n}, \tau \rangle,$$

et $\mathcal{P}_n^\tau$ la fonction de Weierstrass de Λ_n^τ. Si k est un corps, notons $cl.a.(k)$ sa clôture algébrique. Nous rappelons que (voir [26, pp. 316-336]) pour tout corps de courbe elliptique K, d'invariant modulaire j, sur un corps algébriquement clos k de caractéristique 0 sous-corps de $\mathbf{C}$, il existe u et v dans K et des éléments a et b de k tels que $v^2 = 4u^3 - au - b$. Mais nous avons

$$j = 1728\frac{a^3}{a^3 - 27b^2} \in k.$$

Il s'ensuit que le corps k contient $cl.a.(\mathbf{Q}(j))$. Notons j_τ l'invariant modulaire de la courbe elliptique associée à $\frac{\mathbf{C}}{\Lambda_1^\tau}$ et

$$\Delta_\tau = cl.a.(\mathbf{Q}(j_\tau)).$$

Enfin, notons $\mathcal{L}$ le langage des corps et $\mathcal{L}(j_\tau)$ le langage des corps ayant j_τ comme symbole de constante supplémentaire.

Si τ est un nombre complexe algébrique quadratique, k un sous-corps de $\mathbf{C}$ algébriquement clos contenant Δ_τ, et $n > 1$ un entier, soit $\mathbf{P}_n^\tau(k)$ la propriété : *les corps elliptiques* $k(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau\prime})$ *et* $k(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau\prime})$ *ne sont pas élémentairement équivalents dans le langage* $\mathcal{L}(j_\tau)$. Si K est un corps de courbe de genre 1 sur un corps algébriquement clos k de caractéristique 0, avec multiplication complexe et d'invariant modulaire j, et K' un corps de courbe sur k non isomorphe à K, soit $\mathbf{P}_k(K, K')$ la propriété : *les corps elliptiques K et K' ne sont pas élémentairement équivalents dans le langage $\mathcal{L}(j)$.*

Proposition 4.1 . *Si la propriété* $\mathbf{P}_n^\tau(k)$ *est vraie pour tout triplet* (k, τ, n)*, alors la propriété* $\mathbf{P}_k(K, K')$ *est vraie pour tout triplet* (k, K, K').

Démonstration : Voir section 3, prop. 3.6. □

Dans toute la sous-section 4.2, le corps k et le nombre τ seront fixés, il n'est donc plus nécessaire de les faire apparaître dans les notations.

4.2 Résultat principal

Pour tout entier $n \geq 1$, notons E_n le quotient $\frac{\mathbf{C}}{\Lambda_n}$ et C_n la courbe elliptique associée à E_n (voir [46, chap. VI, thm. 5.3, p. 162]). Pour des entiers naturels a, b et p, $p \neq 0$, notons :

$$\begin{aligned}
\Lambda_{a,b}^n &= \langle \frac{1}{n}, \frac{a}{pn} + \frac{b\tau}{p} \rangle \quad \text{si} \quad b \neq 0 \qquad \text{et} \quad \Lambda_{a,0}^n = \langle \frac{a}{pn}, \tau \rangle, \\
\mathcal{I}_p &= \{(a,b) \in \mathbf{N}^2 - \{(0,0)\} \mid 0 \leq a \leq p-1 \quad \text{et} \quad 0 \leq b \leq p-1\}, \\
E_{a,b}^n &= \frac{\mathbf{C}}{\Lambda_{a,b}^n}.
\end{aligned}$$

Soit $C_{a,b}^n$ la courbe elliptique associée à $E_{a,b}^n$.

Lemme 4.2 . *Soit p un nombre premier et soit G un sous-groupe d'ordre p de E_n. Alors il existe un couple $(a,b) \in \mathcal{I}_p$ tel que :*

$$G = \frac{\Lambda_{a,b}^n}{\Lambda_n \bigcap \Lambda_{a,b}^n}.$$

En particulier, il n'y a qu'un nombre fini de sous-groupes d'ordre p de E_n.

Démonstration : Les points d'ordre p de E_n sont précisément les points de la forme :

$$T_{a,b} = \frac{a}{pn} + \frac{b\tau}{p} + \Lambda_n$$

avec $(a, b) \in \mathcal{I}_p$. Soit $G^n_{a,b}$ le groupe engendré par $T_{a,b}$. Nous avons alors :

$$\frac{\Lambda^n_{a,b}}{\Lambda_n \bigcap \Lambda^n_{a,b}} = \begin{cases} \frac{\langle \frac{1}{n}, \frac{a}{pn} + \frac{b\tau}{p} \rangle}{\langle \frac{1}{n}, \tau \rangle \bigcap \langle \frac{1}{n}, \frac{a}{pn} + \frac{b\tau}{p} \rangle} = \{k(\frac{a}{pn} + \frac{b\tau}{p}) + \langle \frac{1}{n}, \tau \rangle \mid k = 1, \ldots, p\} = G^n_{a,b} & \text{si } b \neq 0 \\ \frac{\langle \frac{a}{pn}, \tau \rangle}{\langle \frac{1}{n}, \tau \rangle \bigcap \langle \frac{1}{n}, \frac{a}{pn} + \frac{b\tau}{p} \rangle} = \{k(\frac{a}{pn}) + \langle \frac{1}{n}, \tau \rangle \mid k = 1, \ldots, p\} = G^n_{a,0} & \text{sinon.} \end{cases}$$

□

Si C et C' sont des courbes elliptiques, une isogénie de C vers C' est un morphisme de groupes entre C et C'. Si ϕ est une isogénie, nous noterons deg (ϕ) son degré (voir [46, chap. III, §4]).

Lemme 4.3 . *Soit $\phi\colon C_1 \xrightarrow{\times\alpha^{-1}} C_n$ une isogénie (α^{-1} étant le nombre complexe associé). Soit p un nombre premier tel que p divise le degré de ϕ. Alors il existe un réseau $\Lambda^n_{a,b}$ tel que ϕ se factorise de la manière suivante :*

$$\begin{tikzcd} C_1 \arrow[r, "\lambda", "\times(p\alpha)^{-1}"'] & C^n_{a,b} \arrow[r, "\psi", "\times p"'] & C_n \end{tikzcd}$$

où ψ est une isogénie de degré p.

Démonstration : Soit $\widehat{\phi}\colon C_n \to C_1$ l'isogénie duale de ϕ, et soit d le degré de ϕ ; $\widehat{\phi}$ est donc associée au nombre complexe $d\alpha$, car $\widehat{\phi} \circ \phi$ correspond à la multiplication par d. Soient $f\colon E_1 \xrightarrow{\times\alpha^{-1}} E_n$ et $\widehat{f}\colon E_n \xrightarrow{\times d\alpha} E_1$ les morphismes de groupes associés respectivement aux isogénies ϕ et $\widehat{\phi}$. Nous avons :

$$|\ker \widehat{f}| = \deg \widehat{\phi} = \deg \phi = |\ker f| = \left| \frac{\alpha\Lambda_n}{\Lambda_1} \right| = \left| \frac{\Lambda_n}{\alpha^{-1}\Lambda_1} \right| = |\alpha^{-1}|^2 \times \left| \frac{\langle \frac{1}{n}, \tau \rangle}{\langle 1, \tau \rangle} \right| = n|\alpha^{-1}|^2.$$

Voir [28, chap. 2, §2 et 3] pour l'avant-dernière egalité. Comme p divise le degré de ϕ, p divise aussi $|\ker \widehat{f}|$, donc $\ker \widehat{f}$ contient un sous-groupe d'ordre p, qui est donc d'après le lemme 4.2 de la forme $G^n_{a,b} = \frac{\Lambda^n_{a,b}}{\Lambda_n \bigcap \Lambda^n_{a,b}}$ avec $(a, b) \in \mathcal{I}_p$. Le morphisme de groupes $\widehat{f}$ se factorise donc de manière canonique (ligne du haut) :

$$\begin{tikzcd} E_n \arrow[r, "\widehat{pr}"] & \frac{E_n}{G^n_{a,b}} \arrow[r, "\widehat{\imath}"] \arrow[d, "i"', "\simeq"] & E_1 \\ & E^n_{a,b} & \end{tikzcd}$$

où $\widehat{pr}$ est la projection canonique et donc

$$|\ker \widehat{pr}| = |G^n_{a,b}| = p.$$

Soit

$$\widehat{\psi}\colon C_n \longrightarrow C^n_{a,b} \qquad \text{et} \qquad \widehat{\lambda}\colon C^n_{a,b} \longrightarrow C_1$$

les morphismes de courbes associés respectivement à $i \circ \widehat{pr}$ et à $\widehat{l} \circ i^{-1}$. Nous obtenons alors une factorisation de $\widehat{\phi}$:

$$\begin{tikzcd} C_n \arrow[r, "\widehat{\psi}", "\times 1"'] & C_{a,b}^n \arrow[r, "\widehat{\lambda}", "\times d\alpha"'] & C_1 \end{tikzcd}$$

avec

$$\deg \widehat{\psi} = |\ker (i \circ \widehat{pr})| = |\ker \widehat{pr}| = p.$$

Donc si nous notons ψ le morphisme dual de $\widehat{\psi}$, ψ correspond à la multiplication par p. Nous notons de même λ le morphisme dual de $\widehat{\lambda}$. Nous avons donc la factorisation désirée pour ϕ :

$$\begin{tikzcd} C_1 \arrow[r, "\lambda", "\times (p\alpha)^{-1}"'] & C_{a,b}^n \arrow[r, "\psi", "\times p"'] & C_n. \end{tikzcd}$$

□

Lemme 4.4 . *Nous avons les propriétés suivantes d'homogénéité :*

$$\mathcal{P}(cz, c\Lambda) = \frac{1}{c^2}\mathcal{P}(z,\Lambda), \qquad \mathcal{P}'(cz, c\Lambda) = \frac{1}{c^3}\mathcal{P}(cz, c\Lambda),$$

$$g_2(c\Lambda) = \frac{1}{c^4}g_2(\Lambda), \qquad g_3(c\Lambda) = \frac{1}{c^6}g_3(\Lambda).$$

Démonstration : Voir par exemple [28, chap. 1, §4, pp. 16-17]. □

Nous noterons $\mathcal{E}(\Lambda)$ le corps des fonctions méromorphes ayant pour ensemble de périodes Λ. Nous avons l'égalité suivante (voir [28, chap. 1, §2, thm. 4]) :

$$\mathcal{E}(\Lambda) = \mathbf{C}(\mathcal{P}(.,\Lambda), \mathcal{P}'(.,\Lambda)).$$

En termes de corps, nous obtenons, d'après le lemme 4.3, une factorisation du morphisme de corps $\phi^* \colon \mathcal{E}(\Lambda_n) \longrightarrow \mathcal{E}(\Lambda_1)$,

$$\begin{tikzcd} \mathcal{E}(\Lambda_n) \arrow[r, "\psi^*"] & \mathcal{E}(\Lambda_{a,b}^n) \arrow[r, "\lambda^*"] & \mathcal{E}(\Lambda_1) \end{tikzcd} \qquad (\bigstar)$$

où :

$$(\phi^* f)(z) = f(\frac{z}{\alpha}), \quad (\psi^* f)(z) = f(pz) \quad \text{et} \quad (\lambda^* f)(z) = f(\frac{z}{p\alpha}).$$

Lemme 4.5 . *L'image de* ψ^* *est*

$$\psi^*\mathcal{E}(\Lambda_n) = \mathcal{E}(\frac{1}{p}\Lambda_n).$$

Démonstration : En effet, si $f \in \mathcal{E}(\Lambda_n)$, nous avons, pour tous entiers $r, s \in \mathbf{Z}$:

$$\psi^* f(z + \frac{1}{p}(\frac{r}{n} + s\tau)) = f(pz + \frac{r}{n} + s\tau) = f(pz) = \psi^* f(z),$$

donc $\psi^* f \in \mathcal{E}(\frac{1}{p}\Lambda_n)$. Nous obtenons ainsi l'inclusion $\psi^*\mathcal{E}(\Lambda_n) \subset \mathcal{E}(\frac{1}{p}\Lambda_n)$.

Réciproquement, si $g \in \mathcal{E}(\frac{1}{p}\Lambda_n)$, soit f la fonction méromorphe définie par $f(z) = g(\frac{z}{p})$. Nous avons alors $\psi^* f(z) = f(pz) = g(z)$ et, pour tous entiers $r, s \in \mathbf{Z}$:

$$f(z + \frac{r}{n} + s\tau) = g(\frac{z}{p} + \frac{1}{p}(\frac{r}{n} + s\tau)) = g(\frac{z}{p}) = f(z),$$

donc $f \in \mathcal{E}(\Lambda_n)$. Ceci démontre l'inclusion réciproque. □

Étudions l'extension $\mathcal{E}(\frac{1}{p}\Lambda_n) \subset \mathcal{E}(\Lambda_{a,b}^n)$. Pour cela, nous avons besoin du lemme préliminaire suivant :

Lemme 4.6 . *Soient Λ et Λ' deux réseaux tels que Λ soit sous-réseau de Λ'. Alors $g_2(\Lambda')$ et $g_3(\Lambda')$ sont algébriques sur $\mathbf{Q}(g_2(\Lambda), g_3(\Lambda))$.*

Démonstration : D'après [20, §63, p. 132], il existe une base (ω_1, ω_2) de Λ, et des entiers $r, s \in \mathbf{N}$ non nuls, tels que $(\frac{\omega_1}{rs}, \frac{\omega_2}{r})$ soit une base de Λ'. Notons Λ_s le réseau $\langle \frac{\omega_1}{s}, \omega_2 \rangle$. Nous considérons le diagramme suivant :

$$\begin{array}{ccc}
\Lambda & \subset & \Lambda' \\
\shortparallel & & \shortparallel \\
\langle \omega_1, \omega_2 \rangle & \subset & \langle \frac{\omega_1}{rs}, \frac{\omega_2}{r} \rangle \\
\cap & & \cup \\
\langle \frac{\omega_1}{s}, \omega_2 \rangle & = & \langle \frac{\omega_1}{s}, \omega_2 \rangle \\
\shortparallel & & \shortparallel \\
\Lambda_s & & \Lambda_s
\end{array}$$

Nous savons que $g_i(\Lambda_s)$, pour $i = 2, 3$, est algébrique sur $\mathbf{Q}(g_2(\Lambda), g_3(\Lambda))$ (voir [19, prop. 31, p. 816]). D'après le lemme 4.4, nous avons : $g_i(\Lambda') = r^{2i} g_i(\Lambda_s)$, pour $i = 2, 3$, donc $g_i(\Lambda')$, pour $i = 2, 3$, est aussi algébrique sur $\mathbf{Q}(g_2(\Lambda), g_3(\Lambda))$. □

Pour un réseau Λ, si j_Λ désigne l'invariant modulaire de la courbe elliptique associée à $\frac{\mathbf{C}}{\Lambda}$, nous avons :

$$cl.a.(\mathbf{Q}(g_2(\Lambda), g_3(\Lambda))) = cl.a.(\mathbf{Q}(j_\Lambda)).$$

Voir par exemple [26, pp. 316-336]. Notons

$$j = j_{\Lambda_1} \qquad \text{et} \qquad \Delta = cl.a.(\mathbf{Q}(j)).$$

Corollaire 4.7 . *Les nombres complexes $g_2(\Lambda^n_{a,b})$ et $g_3(\Lambda^n_{a,b})$ sont éléments de Δ.*

Démonstration : L'égalité

$$\lambda^* \mathcal{E}(\Lambda^n_{a,b}) = \mathcal{E}(p\alpha\Lambda^n_{a,b})$$

se démontre de façon analogue à la démonstration du lemme 4.5. Donc nous avons, d'après ($\bigstar$),

$$\mathcal{E}(p\alpha\Lambda^n_{a,b}) \subset \mathcal{E}(\Lambda_1),$$

ou, en termes de réseaux :

$$\Lambda_1 \subset p\alpha\Lambda^n_{a,b}.$$

Donc par le lemme 4.6, pour $i = 2, 3$, le nombre $g_i(p\alpha\Lambda^n_{a,b})$ est algébrique sur

$$\mathbf{Q}(g_2(\Lambda_1), g_3(\Lambda_1)).$$

Mais nous avons, d'après le lemme 4.4,

$$g_i(p\alpha\Lambda^n_{a,b}) = (\frac{1}{p\alpha})^{2i} g_i(\Lambda^n_{a,b}), \quad \text{pour} \quad i = 2, 3.$$

D'après ($\bigstar$), le nombre α^{-1} est élément de Hom (E_1, E_n), donc d'après la proposition 4.15 (voir section 4.3), α est algébrique sur $\mathbf{Q}$. Par conséquent, $g_2(\Lambda^n_{a,b})$ et $g_3(\Lambda^n_{a,b})$ sont algébriques sur $\mathbf{Q}(g_2(\Lambda_1), g_3(\Lambda_1))$. □

Notons $\mathcal{P}^n_{a,b}$ la fonction de Weierstrass du réseau $\Lambda^n_{a,b}$.

Lemme 4.8 . *Il existe une fraction rationnelle F, à coefficients dans Δ, telle que :*

$$\psi^* \mathcal{P}_n = F(\mathcal{P}^n_{a,b}).$$

Démonstration : D'après le lemme 4.5 et (★), nous avons

$$\psi^*\mathcal{E}(\Lambda_n) = \mathcal{E}(\frac{1}{p}\Lambda_n) \subset \mathcal{E}(\Lambda^n_{a,b}),$$

et donc le réseau $\Lambda^n_{a,b}$ est inclus dans le réseau $\frac{1}{p}\Lambda_n$. Nous ne pouvons pas pour l'instant appliquer [19, prop. 30, p. 815], mais nous nous y ramenons en constatant la présence d'un réseau intermédiaire Γ; dans les deux cas : $b = 0$ et $b \neq 0$;

$$\begin{array}{ccccccccc}
\text{si } b=0 & \Lambda^n_{a,b} & = & \langle \frac{a}{np}, \tau \rangle & \subset & \langle \frac{1}{np}, \frac{\tau}{p} \rangle & = & \frac{1}{p}\Lambda_n \\
 & & & \cap & & \cup & & \\
 & \Gamma & = & \langle \frac{a}{np}, \frac{\tau}{p} \rangle & = & \langle \frac{a}{np}, \frac{\tau}{p} \rangle & = & \Gamma
\end{array}$$

$$\begin{array}{ccccccccc}
\text{si } b\neq 0 & \Lambda^n_{a,b} & = & \langle \frac{1}{n}, \frac{a}{np} + \frac{b\tau}{p} \rangle & \subset & \langle \frac{1}{np}, \frac{\tau}{p} \rangle & = & \frac{1}{p}\Lambda_n \\
 & & & \cap & & \cup & & \\
 & \Gamma & = & \langle \frac{1}{np}, \frac{a}{np} + \frac{b\tau}{p} \rangle & = & \langle \frac{1}{np}, \frac{b\tau}{p} \rangle & = & \Gamma
\end{array}$$

puis en considérant pour chaque inclusion les images des réseaux par la similitude qui convient. Par exemple, lorsque $b = 0$, pour l'inclusion de gauche, nous multiplions les deux réseaux par $\frac{1}{\tau}$ et nous appliquons [19, prop. 30, p. 815], à l'extension :

$$\mathcal{E}\left(\langle \frac{a}{np\tau}, \frac{1}{p} \rangle\right) \subset \mathcal{E}\left(\langle \frac{a}{np\tau}, 1 \rangle\right).$$

Il existe donc une fraction rationnelle G' à coefficients dans

$$cl.a.(\mathbf{Q}(g_2(\frac{1}{\tau}\Gamma), g_3(\frac{1}{\tau}\Gamma))) = cl.a.(\mathbf{Q}(g_2(\Gamma), g_3(\Gamma)))$$

(l'égalité provenant du lemme 4.4) telle que

$$\mathcal{P}\left(., \frac{1}{\tau p}\Lambda_n\right) = G' \circ \mathcal{P}\left(., \frac{1}{\tau}\Gamma\right).$$

La propriété d'homogénéité des fonctions de Weierstrass (voir lemme 4.4) nous permet de conclure qu'il existe une fraction rationnelle G à coefficients dans

$$cl.a.\left(\mathbf{Q}(g_2(\Gamma), g_3(\Gamma))\right)$$

telle que

$$\mathcal{P}\left(., \frac{1}{p}\Lambda_n\right) = G \circ \mathcal{P}\left(., \Gamma\right).$$

En effet, pour tout $z \in \mathbf{C}$, nous avons :

$$\mathcal{P}\left(\tau z, \frac{1}{p}\Lambda_n\right) = \frac{1}{\tau^2}\mathcal{P}\left(z, \frac{1}{\tau p}\Lambda_n\right) = \frac{1}{\tau^2}G' \circ \mathcal{P}\left(z, \frac{1}{\tau}\Gamma\right) = \frac{1}{\tau^2}G'(\tau^2\mathcal{P}(\tau z, \Gamma)).$$

Nous pouvons donc poser

$$G(X) = \frac{1}{\tau^2}G'(\tau^2 X).$$

En procédant de même pour les trois autres extensions, nous pouvons affirmer qu'il existe des fractions rationnelles G à coefficients dans $cl.a.(\mathbf{Q}(g_2(\Gamma), g_3(\Gamma)))$, et H à coefficients dans $cl.a.(\mathbf{Q}(g_2(\Lambda^n_{a,b}), g_3(\Lambda^n_{a,b})))$, telles que nous ayons :

$$\mathcal{P}(., \frac{1}{p}\Lambda_n) = G \circ \mathcal{P}(., \Gamma) \qquad \text{et} \qquad \mathcal{P}(., \Gamma) = H \circ \mathcal{P}^n_{a,b}.$$

Or nous avons :

$$(\psi^*\mathcal{P}_n)(z) = \mathcal{P}_n(pz) = \mathcal{P}(pz, \Lambda_n) = \mathcal{P}(pz, p.\frac{1}{p}\Lambda_n) = \frac{1}{p^2}\mathcal{P}(z, \frac{1}{p}\Lambda_n),$$

et il s'ensuit que :

$$\psi^*\mathcal{P}_n = \frac{1}{p^2}\mathcal{P}(., \frac{1}{p}\Lambda_n) = \frac{1}{p^2}G \circ H \circ \mathcal{P}^n_{a,b}.$$

De plus, d'après le lemme 4.6, $g_2(\Gamma)$ et $g_3(\Gamma)$ sont algébriques sur $\mathbf{Q}(g_2(\Lambda^n_{a,b}), g_3(\Lambda^n_{a,b}))$, donc il en est de même des coefficients du polynôme $\frac{1}{p^2}G \circ H$. Le corollaire 4.7 permet alors de conclure. □

Le lemme 4.8 est l'analogue de [19, prop. 30, p. 815], qui permet de démontrer [19, prop. 32, p. 817]. Nous déduisons exactement de la même façon du lemme 4.8 le corollaire suivant, analogue de [19, prop. 32, p. 817] :

Corollaire 4.9 . *Soit k un sous-corps de $\mathbf{C}$, extension de Δ.*

1. *les corps $\Delta(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)$ et $k(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)$ sont sous-corps respectivement de $\Delta(\mathcal{P}^n_{a,b}, \mathcal{P}^{n'}_{a,b})$ et de $k(\mathcal{P}^n_{a,b}, \mathcal{P}^{n'}_{a,b})$.*
2. *la fonction de Weierstrass $\mathcal{P}^n_{a,b}$ est élément primitif de $\Delta(\mathcal{P}^n_{a,b}, \mathcal{P}^{n'}_{a,b})$ sur $\Delta(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)$, de $k(\mathcal{P}^n_{a,b}, \mathcal{P}^{n'}_{a,b})$ sur $k(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)$ et de $\mathbf{C}(\mathcal{P}^n_{a,b}, \mathcal{P}^{n'}_{a,b})$ sur $\mathbf{C}(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)$.*
3. *Tout polynôme minimal de $\mathcal{P}^n_{a,b}$ sur $\Delta(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)$ est polynôme minimal de $\mathcal{P}^n_{a,b}$ sur $k(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)$ et sur $\mathbf{C}(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)$. Il existe donc un polynôme $P^n_{a,b}(X, Y, Z)$ à coefficients dans Δ, tel que $P^n_{a,b}(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n, Z)$ soit polynôme minimal de $\mathcal{P}^n_{a,b}$ sur $\psi^*\mathcal{E}(\Lambda_n)$.*

Notons :

$$\mathrm{Hom}\,(E_1, E_n) = \{\alpha \in \mathbf{C} \mid \alpha\Lambda_1 \subset \Lambda_n\}$$

et $\mathrm{End}\,E_n = \mathrm{Hom}\,(E_n, E_n)$. Le corps k et le nombre τ ayant été fixés précédemment, nous avons les deux résultats suivants :

Théorème 4.10 .[Duret] *Si les réseaux $\mathrm{Hom}\,(E_1, E_n)$ et $\mathrm{End}\,E_1$ sont égaux, alors les corps elliptiques $k(\mathcal{P}_n, \mathcal{P}_n{}')$ et $k(\mathcal{P}_1, \mathcal{P}_1{}')$ ne sont pas élémentairement équivalents dans le langage $\mathcal{L}(j)$.*

Démonstration : Voir la remarque [18, rem. 37, p. 821] relative à [18, thm. 35, p. 818]. □

Théorème 4.11 . *S'il existe un entier $p \in \mathbf{N}$ tel que $1 \leq p < n$ et tel que les réseaux $\mathrm{Hom}\,(E_1, E_n)$ et $\mathrm{Hom}\,(E_1, E_p)$ soient égaux, alors les corps elliptiques $k(\mathcal{P}_n, \mathcal{P}_n{}')$ et $k(\mathcal{P}_1, \mathcal{P}_1{}')$ ne sont pas élémentairement équivalents dans le langage $\mathcal{L}(j)$.*

Démonstration : Voir section 3, thm. 3.9. □

Notons $R_n(X,Y)$ le polynôme

$$R_n(X,Y) = Y^2 - 4X^3 + g_2(\Lambda_n)X + g_3(\Lambda_n) \in \Delta[X,Y]$$

(appliquer le lemme 4.6 en choisissant $\Lambda = \Lambda_1$ et $\Lambda' = \Lambda_n$ pour voir que les coefficients de $R_n(X,Y)$ sont dans Δ). Voici maintenant le résultat principal de cet article :

Théorème 4.12 . *S'il existe un nombre premier p tel que, pour toute isogénie $\phi \in \mathrm{Hom}\,(C_1, C_n)$, p divise le degré de ϕ, alors les corps elliptiques $k(\mathcal{P}_n, \mathcal{P}_n{}')$ et $k(\mathcal{P}_1, \mathcal{P}_1{}')$ ne sont pas élémentairement équivalents dans le langage $\mathcal{L}(j)$.*

Démonstration : Nous allons construire une formule Θ_n du langage $\mathcal{L}(j)$ qui est vraie dans le corps $k(\mathcal{P}_n, \mathcal{P}_n{}')$ tandis qu'elle est fausse dans $k(\mathcal{P}_1, \mathcal{P}_1{}')$. D'après [19, prop. 33, p. 818], il suffit de trouver une telle formule dans le langage $\mathcal{L}(\Delta)$. D'après [18, prop. 10, p. 950], il existe une formule C du langage $\mathcal{L}(\Delta)$ définissant k dans $k(\mathcal{P}_n, \mathcal{P}_n{}')$ et dans $k(\mathcal{P}_1, \mathcal{P}_1{}')$, et $\mathbf{C}$ dans $\mathbf{C}(\mathcal{P}_n, \mathcal{P}_n{}')$ et dans $\mathbf{C}(\mathcal{P}_1, \mathcal{P}_1{}')$. Soit Θ_n la formule

$$\exists x, y \Big(\neg C(x) \wedge R_n(x,y) = 0 \wedge \forall z \bigwedge_{(a,b)\in\mathcal{I}_p} P^n_{a,b}(x,y,z) \neq 0 \Big)$$

où $P^n_{a,b}(X,Y,Z) \in \Delta[X,Y,Z]$ est le polynôme défini dans le lemme 4.9(3).

Montrons que $k(\mathcal{P}_n, \mathcal{P}'_n)$ satisfait la formule Θ_n. Choisissons $x = \mathcal{P}_n$ et $y = \mathcal{P}'_n$. Supposons qu'il existe un couple (a,b) de $\mathcal{I}_p$ et un élément z de $k(\mathcal{P}_n, \mathcal{P}'_n)$ tels que

$$P^n_{a,b}(\mathcal{P}_n, \mathcal{P}'_n, z) = P^n_{a,b}(x,y,z) = 0.$$

Alors

$$\psi^*(P^n_{a,b}(\mathcal{P}_n, \mathcal{P}'_n, z)) = 0,$$

et nous avons donc

$$[k(\mathcal{P}^n_{a,b}, \mathcal{P}^{n'}_{a,b})\colon k(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)] = [\mathcal{E}(\Lambda^n_{a,b})\colon \psi^*\mathcal{E}(\Lambda_n)] = 1.$$

Ceci est absurde puisque ψ est degré p (voir ($\bigstar$)).

Montrons que $k(\mathcal{P}_1, \mathcal{P}'_1)$ satisfait la formule $\neg\Theta_n$, c'est à dire :

$$k(\mathcal{P}_1, \mathcal{P}'_1) \models \forall x, y \Big(\neg C(x) \wedge R_n(x,y) = 0 \to \exists z \bigvee_{(a,b)\in\mathcal{I}_p} P^n_{a,b}(x,y,z) = 0 \Big).$$

Soient donc u et v des éléments de $k(\mathcal{P}_1, \mathcal{P}'_1)$, avec $u \notin k$, qui annulent le polynôme $R_n(X,Y)$. Nous cherchons un élément w de $k(\mathcal{P}_1, \mathcal{P}'_1)$ tel qu'il existe un couple $(a,b) \in \mathcal{I}_p$ pour lequel $P^n_{a,b}(u,v,w) = 0$. S'il existe un tel w, il est algébrique sur $\Delta(u,v) \subset k(\mathcal{P}_1, \mathcal{P}'_1)$. Mais $k(\mathcal{P}_1, \mathcal{P}'_1)$ est algébriquement clos dans $\mathbf{C}(\mathcal{P}_1, \mathcal{P}'_1)$ (voir [19, prop. 32(3) et sa démonstration, p. 817]), donc il existe un tel w dans $k(\mathcal{P}_1, \mathcal{P}'_1)$ si et seulement s'il en existe un dans $\mathbf{C}(\mathcal{P}_1, \mathcal{P}'_1)$. Les conditions sur u et v nous donnent un isomorphisme et un morphisme de corps :

$$\rho^*\colon \mathbf{C}(\mathcal{P}_n, \mathcal{P}'_n) \xrightarrow{\sim} \mathbf{C}(u,v) \subset \mathbf{C}(\mathcal{P}_1, \mathcal{P}'_1)$$

avec $\rho^*(\mathcal{P}_n) = u$ et $\rho^*(\mathcal{P}'_n) = v$. Donc il existe des nombres complexes α et β, $\alpha \neq 0$, tels que pour toute fonction $f \in \mathbf{C}(\mathcal{P}_n, \mathcal{P}'_n)$, nous ayons :

$$(\rho^* f)(z) = f(\alpha^{-1} z + \beta)$$

(voir [20, §90, pp. 195-196]). Soit $\rho\colon C_1 \to C_n$ le morphisme de courbes associé à ρ^*, et $r\colon E_1 \to E_n$ le morphisme associé à ρ; il est donc donné par

$$r(z) = \alpha^{-1}z + \beta.$$

Si β n'est pas élément de Λ_n, r n'est pas un morphisme de groupes et donc ρ n'est pas une isogénie. Dans ce cas, nous composons avec la translation $t_{-\alpha\beta}\colon E_1 \to E_1$ donnée par

$$t_{-\alpha\beta}(z) = z - \alpha\beta.$$

Appelons f la composée $r \circ t_{-\alpha\beta}$. Nous avons alors :

$$f(z) = r \circ t_{-\alpha\beta}(z) = r(z - \alpha\beta) = \alpha^{-1}(z - \alpha\beta) + \beta = \alpha^{-1}z.$$

Notons $\tau_{-\alpha\beta}$ le morphisme de courbes associé à $t_{-\alpha\beta}$. Soit $\phi = \rho \circ \tau_{-\alpha\beta}$ le morphisme de courbes associé à f. Donc $\phi\colon C_1 \to C_n$ est une isogénie, et par hypothèse son degré est divisible par p. D'après le lemme 4.3, il existe donc un couple $(a, b) \in \mathcal{I}_p$ tel que ϕ se factorise de la manière suivante, avec $\deg \psi = p$,

$$\begin{tikzcd} C_1 \arrow[r, "\lambda", "\times(p\alpha)^{-1}"'] & C^n_{a,b} \arrow[r, "\psi", "\times p"'] & C_n. \end{tikzcd}$$

Ceci nous donne une factorisation pour $\rho = \psi \circ \lambda \circ (\tau_{-\alpha\beta})^{-1} = \psi \circ \lambda \circ \tau_{\alpha\beta}$,

$$\begin{tikzcd} C_1 \arrow[r, "\tau_{\alpha\beta}"] & C_1 \arrow[r, "\lambda"] & C^n_{a,b} \arrow[r, "\psi"] & C_n, \end{tikzcd}$$

et en termes de corps, nous obtenons une factorisation de ρ^*,

$$\begin{tikzcd} \mathcal{E}(\Lambda_n) \arrow[r, "\psi^*"] & \mathcal{E}(\Lambda^n_{a,b}) \arrow[r, "\lambda^*"] & \mathcal{E}(\Lambda_1) \arrow[r, "\tau^*_{\alpha\beta}"] & \mathcal{E}(\Lambda_1). \end{tikzcd}$$

L'élément que nous cherchions est $w = \tau^*_{\alpha\beta} \circ \lambda^*(\mathcal{P}^n_{a,b})$. En effet, nous avons :

$$\begin{aligned} P^n_{a,b}(u, v, w) &= P^n_{a,b}(\rho^*\mathcal{P}_n, \rho^*\mathcal{P}'_n, \tau^*_{\alpha\beta} \circ \lambda^*(\mathcal{P}^n_{a,b}) \\ &= \tau^*_{\alpha\beta} \circ \lambda^* P^n_{a,b}(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n, \mathcal{P}^n_{a,b}) \\ &= 0. \end{aligned}$$

□

Pierce a démontré la proposition suivante (voir [37, thm. 8 et thm. 10 ensemble]) :

Proposition 4.13 . *Les anneaux d'endomorphismes* End (E_1) *et* End (E_n) *ne sont pas égaux si et seulement s'il existe un nombre premier p qui divise le degré de toute isogénie $\Phi \in$* Hom (C_1, C_n).

Nous obtenons donc, en combinant le théorème 4.12 et la proposition 4.13, le théorème annoncé en introduction :

Théorème 4.14 . *Si les anneaux d'endomorphismes* End (E_1) *et* End (E_n) *sont distincts, alors les corps elliptiques $k(\mathcal{P}_n, \mathcal{P}_n{}')$ et $k(\mathcal{P}_1, \mathcal{P}_1{}')$ ne sont pas élémentairement équivalents dans le langage $\mathcal{L}(j)$.*

4.3 Limites et portée des résultats

Soit AX^2+BX+C un polynôme dont τ est la racine, où $A \in \mathbf{N}$ est non nul, et $B, C \in \mathbf{Z}$ sont tels que $A \wedge B \wedge C = 1$ (par la suite, le symbole $\wedge$ désignera toujours le plus grand diviseur commun positif). Si $\bar{\tau}$ désigne la racine conjuguée à τ, nous avons bien sûr

$$\tau\bar{\tau} = \frac{C}{A} \qquad \text{et} \qquad \tau + \bar{\tau} = -\frac{B}{A}.$$

Notons

$$\delta_n = A \wedge nB \wedge nC = A \wedge n \qquad \text{et} \qquad \delta'_n = A \wedge nB \wedge n^2C.$$

Il est immédiat, d'après la définition de Hom, que pour tout entier $n \geq 1$, nous avons

$$\mathrm{End}\, E_1 \subset \mathrm{Hom}\,(E_1, E_n) \qquad \text{et} \qquad \mathrm{End}\, E_n \subset \mathrm{Hom}\,(E_1, E_n).$$

Proposition 4.15 . *Pour tout entier $n \geq 1$, nous avons :*

$$\mathrm{Hom}\,(E_1, E_n) = \langle 1, \frac{A}{\delta_n}\bar{\tau}\rangle$$

Démonstration : Voir section 3, prop. 3.1. □

Etant donnés deux entiers $k, k' \in \mathbf{N}$, nous avons :

$$\langle 1, k\tau\rangle = \langle 1, k'\tau\rangle \Longleftrightarrow |k| = |k'|.$$

En effet, si les réseaux $\langle 1, k\tau\rangle$ et $\langle 1, k'\tau\rangle$ sont égaux, alors il existe des entiers $a, b \in \mathbf{Z}$ tels que $k\tau = ak'\tau$ et $k'\tau = bk\tau$, donc nous avons $|a| = |b| = 1$.

Corollaire 4.16 . *Pour tout entier $n \geq 1$, nous avons :*

1. $\mathrm{End}\, E_1 = \langle 1, A\tau\rangle = \langle 1, A\bar{\tau}\rangle$
2. $\mathrm{End}\, E_n = \langle 1, \frac{An}{\delta'_n}\tau\rangle = \langle 1, \frac{An}{\delta'_n}\bar{\tau}\rangle$
3. *Si* $\mathrm{End}\, E_1 = \mathrm{End}\, E_n$, *alors* $n|A$.
4. *Si* $\mathrm{End}\, E_1 = \mathrm{End}\, E_n$, *alors* $\mathrm{Hom}\,(E_1, E_n) = \langle 1, \frac{A}{n}\bar{\tau}\rangle$.

Démonstration :

1. La première égalité vient du fait que $A \wedge B \wedge C = 1$. Pour la seconde, nous remarquons que
$$\langle 1, A\bar{\tau}\rangle = \langle 1, -B - A\tau\rangle = \langle 1, A\tau\rangle.$$

2. Nous avons la première égalité car
$$\mathrm{End}\, E_n = \mathrm{End}\left(\frac{\mathbf{C}}{\langle 1, n\tau\rangle}\right)$$
et le polynôme $AX^2 + BnX + Cn^2$ s'annule en $n\tau$. Il faut diviser par δ'_n pour que les coefficients soient premiers entre eux. Nous concluons grâce à (1). Pour obtenir la seconde égalité, nous remarquons que
$$\langle 1, \frac{An}{\delta'_n}\tau\rangle = \langle 1, \frac{n}{\delta'_n}(-B - A\bar{\tau})\rangle = \langle 1, \frac{n}{\delta'_n}A\bar{\tau}\rangle,$$
car $\frac{nB}{\delta'_n}$ est un entier.

3. Si les réseaux $\mathrm{End}\, E_1$ et $\mathrm{End}\, E_n$ sont égaux, alors $\frac{An}{\delta'_n}$ est égal à $\pm A$. Les entiers n et δ'_n étant strictement positifs, nous avons
$$n = \delta'_n = A \wedge nB \wedge n^2C,$$
et donc n divise A.

4. Si les réseaux $\mathrm{End}\, E_1$ et $\mathrm{End}\, E_n$ sont égaux, alors d'après (3), n divise A, donc nous avons
$$\delta_n = n(\frac{A}{n} \wedge B \wedge C) = n,$$
car $\frac{A}{n} \wedge B \wedge C = 1$.

□

Proposition 4.17 . *L'application*
$$\begin{array}{rcl} \{p \in \mathbf{N}^* \mid p \text{ divise } A\} & \longrightarrow & \{\mathrm{Hom}\,(E_1, E_p) \mid p \in \mathbf{N}^*\} \\ p & \longmapsto & \mathrm{Hom}\,(E_1, E_p) \end{array}$$
est une bijection. En particulier, la cardinal de l'ensemble $\{\mathrm{Hom}\,(E_1, E_p) \mid p \in \mathbf{N}^*\}$ *est le nombre de diviseurs de* A.

Démonstration : Voir section 3, cor. 3.5. □

Par conséquent, nous pouvons énoncer le théorème 4.11 de la manière suivante :

Théorème 4.18 . *Si* n *ne divise pas* A*, alors les corps elliptiques* $k(\mathcal{P}_n, \mathcal{P}_n{}')$ *et* $k(\mathcal{P}_1, \mathcal{P}_1{}')$ *ne sont pas élémentairement équivalents dans le langage* $\mathcal{L}(j)$.

Soient $m, r, s, d \in \mathbf{Z}$ tels que $m \geq 1$, $s \neq 0$, $d \geq 1$ et non divisible par un carré, et tels que
$$\tau = \frac{1}{m}(r + is\sqrt{d}).$$
Notons $D = r^2 + ds^2$ et $e = m^2 \wedge 2rm \wedge D$.

Proposition 4.19 . *Nous pouvons choisir* $A = \frac{m^2}{e}$, $B = \frac{-2rm}{e}$ *et* $C = \frac{D}{e}$ *comme coefficients entiers premiers entre eux du polynôme minimal de* τ.

Démonstration : Montrons que $m^2\tau^2 - 2rm\tau + D = 0$.
Nous avons $\tau^2 = \frac{1}{m^2}(r^2 + 2ris\sqrt{d} - ds^2)$. Nous en déduisons que
$$\begin{aligned} &m^2\tau^2 - 2rm\tau + D = \\ &\qquad m^2\frac{1}{m^2}(r^2 + 2ris\sqrt{d} - ds^2) - 2rm\frac{1}{m}(r + is\sqrt{d}) + D = \\ &\qquad\qquad r^2 + 2ris\sqrt{d} - ds^2 - 2r(r + is\sqrt{d}) + r^2 + ds^2 = 0. \end{aligned}$$
Donc le polynôme $\frac{m^2}{e}X^2 - \frac{2rm}{e}X + \frac{D}{e}$ s'annule en τ et a bien ses coefficients premiers entre eux. □

Exemples 4.20 . Dans les deux exemples suivants, nous ne faisons que les calculs qui nous permettront de mieux apprécier le champ d'action et les limites des théorèmes 4.10, 4.11 et 4.12.

1. Pour $\tau = \frac{1}{2} + i = \frac{1}{2}(1+2i)$, nous trouvons $D = 5$, $e = 1$, $A = 4$, $B = -4$, $C = 5$, et donc nous avons $\delta_1 = 1$, $\delta_2 = 2$, $\delta_4 = 4$, $\delta'_2 = \delta'_4 = 4$.

Nous en déduisons que :

$\mathrm{End}\, E_1 = \langle 1, 4i\rangle$, $\mathrm{Hom}\,(E_1, E_2) = \langle 1, 2i\rangle$, $\mathrm{Hom}\,(E_1, E_4) = \langle 1, i\rangle$, $\mathrm{End}\, E_2 = \langle 1, 2i\rangle$ et $\mathrm{End}\, E_4 = \mathrm{End}\, E_1$.

2. Pour $\tau = \frac{1}{6}(2 + 5i\sqrt{2})$, nous trouvons $D = 54$, $e = 6$, $A = 6$, $B = -4$, $C = 9$, et donc on a $\delta_2 = \delta'_2 = 2$, $\delta_3 = \delta'_3 = 3$, $\delta_6 = \delta'_6 = 6$.

Nous en déduisons que :

$\mathrm{End}\, E_1 = \langle 1, 5i\sqrt{2}\rangle$, $\mathrm{Hom}\,(E_1, E_2) = \langle 1, 2i\rangle$, $\mathrm{Hom}\,(E_1, E_4) = \langle 1, i\rangle$, $\mathrm{End}\, E_2 = \langle 1, \frac{5}{2}i\sqrt{2}\rangle$, $\mathrm{Hom}\,(E_1, E_3) = \langle 1, \frac{1}{3}(2 - 5i\sqrt{2})\rangle$, $\mathrm{Hom}\,(E_1, E_6) = \langle 1, \frac{1}{6}(2 - 5i\sqrt{2})\rangle$, et $\mathrm{End}\, E_2 = \mathrm{End}\, E_3 = \mathrm{End}\, E_6 = \mathrm{End}\, E_1$.

D'après le corollaire 4.16(3), si les réseaux $\mathrm{End}\,(E_1)$ et $\mathrm{End}\,(E_n)$ sont égaux, alors n est un diviseur de A. Par conséquent, le théorème 4.12, tout comme 4.11, donne une formule Θ_n pour tous les entiers $n \in \mathbf{N}$ qui ne divisent pas A. Mais comme nous pouvons le voir dans l'exemple 4.20(1), la réciproque de l'item (3) du corollaire 4.16 est fausse. En effet, dans cet exemple, nous trouvons $A = 4$ et $\mathrm{End}\,(E_1) \neq \mathrm{End}\,(E_2)$. Le théorème 4.12 donne dans cet exemple une des deux formules qui n'était pas donnée par le théorème 4.11, soit la formule Θ_2. Par contre, il n'apporte rien de nouveau pour $\tau = \frac{1}{6}(2 + 5i\sqrt{2})$, puisque dans cet exemple, nous avons $A = 6$ et $\mathrm{End}\,(E_1) = \mathrm{End}\,(E_2) = \mathrm{End}\,(E_3) = \mathrm{End}\,(E_6)$.

Si p est un nombre premier, notons $E^n_{a,b}(p)$ le quotient $\frac{\mathbf{C}}{p\Lambda^n_{a,b}}$.

Proposition 4.21 . *Nous avons l'équivalence suivante :*

$$\mathrm{End}\,(E_1) \neq \mathrm{End}\,(E_n) \Longleftrightarrow \exists p \text{ premier} \quad \mathrm{Hom}\,(E_1, E_n) \subset \bigcup_{(a,b)\in\mathcal{I}_p} \mathrm{Hom}\,(E_1, E^n_{a,b}(p)).$$

Démonstration :
$\mathrm{End}\,(E_1) \neq \mathrm{End}\,(E_n)$

$$\begin{aligned}
&\Longleftrightarrow \quad \exists p \text{ premier } \forall \Phi \in \mathrm{Hom}\,(C_1, C_n),\ p | \deg(\Phi)\\
&\Longleftrightarrow \quad \exists p \text{ premier } \forall \alpha^{-1} \in \mathrm{Hom}\,(E_1, E_n),\ \exists (a,b) \in \mathcal{I}_p,\ (p\alpha)^{-1}\Lambda_1 \subset \Lambda^n_{a,b}\\
&\Longleftrightarrow \quad \exists p \text{ premier } \forall \beta \in \mathrm{Hom}\,(E_1, E_n),\ \exists (a,b) \in \mathcal{I}_p,\ \beta\Lambda_1 \subset p\Lambda^n_{a,b}\\
&\Longleftrightarrow \quad \exists p \text{ premier } \forall \beta \in \mathrm{Hom}\,(E_1, E_n),\ \exists (a,b) \in \mathcal{I}_p,\ \beta \in \mathrm{Hom}\,(\tfrac{\mathbf{C}}{\Lambda_1}, \tfrac{\mathbf{C}}{p\Lambda^n_{a,b}})\\
&\Longleftrightarrow \quad \exists p \text{ premier } \forall \beta \in \mathrm{Hom}\,(E_1, E_n),\ \beta \in \textstyle\bigcup_{(a,b)\in\mathcal{I}_p} \mathrm{Hom}\,(E_1, E^n_{a,b}(p))\\
&\Longleftrightarrow \quad \exists p \text{ premier, } \mathrm{Hom}\,(E_1, E_n) \subset \textstyle\bigcup_{(a,b)\in\mathcal{I}_p} \mathrm{Hom}\,(E_1, E^n_{a,b}(p)).
\end{aligned}$$

La première équivalence n'est autre que la proposition 4.13. La seconde vient du lemme 4.3. Pour la troisième, nous posons $\beta = \alpha^{-1}$. □

Nous pouvons donc énoncer les hypothèses des théorèmes 4.10, 4.11 et 4.12 de la manière suivante :

théorème 4.10 :		$\mathrm{Hom}\,(E_1, E_n) \subset \mathrm{Hom}\,(E_1, E_1)$	(1)
théorème 4.11 :	$\exists p < n$	$\mathrm{Hom}\,(E_1, E_n) \subset \mathrm{Hom}\,(E_1, E_p)$	(2)
théorème 4.12 :	$\exists p$ premier	$\mathrm{Hom}\,(E_1, E_n) \subset \bigcup_{(a,b)\in\mathcal{I}_p} \mathrm{Hom}\,(E_1, E^n_{a,b}(p))$	(3)

Nous avons bien sûr (1) $\Rightarrow$ (2). Nous avons aussi (2) $\Rightarrow$ (3) d'après la remarque qui précède la proposition 4.21. Nous pouvons aussi les énoncer d'un point de vue arithmétique :

théorème 4.10 :	n et A sont premiers entre eux	
théorème 4.11 :	n ne divise pas A	
théorème 4.12 :	$n \neq A \wedge nB \wedge n^2C$	$(\bullet)$

où $(\bullet)$ se déduit directement du corollaire 4.16 (1 et 2).

Part II

AN ANALOGUE OF HILBERT'S TENTH PROBLEM FOR p-ADIC GLOBAL MEROMORPHIC FUNCTIONS

5 Sketch of the proof

Let $\mathcal{M}_p$ denote the field of global meromorphic functions on the p-adic complex plain $\mathbf{C}_p$ (the analogue of the complex plain in the p-adic case: $\mathbf{C}_p$ is complete and algebraically closed). We obtain the main theorem 1.2 by studying the solutions over $\mathcal{M}_p$ of equations of the form:

$$\text{(MD)} \qquad (z^3+\delta z^2+z)y^2 = x^3+\delta x^2+x,$$

where z is the independent variable, x and y are functions of z, and δ is a constant in $\mathbf{C}_p - \{\pm 2\}$, so that Equation (MD) defines the affine part of an elliptic curve $\mathcal{E}^*$. These curves have been introduced by Y. Manin and J. Denef.

More precisely, we show that Equation (MD) has only rational solutions over $\mathcal{M}_p$ (Theorem 8.24). The rational solutions have been studied by J. Denef in [11]. For δ fixed, let $\mathcal{E}$ denote the elliptic curve with affine equation

$$(1) \qquad s^2 = z^3+\delta z^2+z.$$

We will use the symbols $\oplus$ and $\ominus$ (resp. $\overset{*}{\oplus}$ and $\overset{*}{\ominus}$) for the addition law of $\mathcal{E}$ (resp. of $\mathcal{E}^*$). Note that if (z,s) is a point on the elliptic curve $\mathcal{E}$, then, to any point (x,y) of $\mathcal{E}^*$ corresponds the point (x,sy) of $\mathcal{E}$. For any n in the ring of endomorphisms of $\mathcal{E}^*$, define

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

Equivalently, we could define x_n and y_n by $(x_n, sy_n) = n(z,s)$, where addition is meant on $\mathcal{E}$. J. Denef proved that the rational solutions of Equation (MD) are of the form $(x_n,y_n)\overset{*}{\oplus}(a,b)$, where (a,b) is a point of order 1 or 2 on $\mathcal{E}$. Because the quotient $\frac{x_n}{zy_n}$ takes the value $\pm n$ at 0, we can conclude that integers are definable in $\mathcal{M}_p$.

Our starting point for the investigation of the solutions over $\mathcal{M}_p$ of Equation (MD) comes from the following property of the rational solutions: for any integer n, we have

$$x_{2n}(z^{-1}) = x_{2n}(z) \qquad \text{and} \qquad y_{2n}(z^{-1}) = -z^2 y_{2n}(z),$$

$$x_{2n+1}(z^{-1}) = x_{2n+1}^{-1}(z) \qquad \text{and} \qquad y_{2n+1}(z^{-1}) = z^2\frac{y_{2n+1}}{x_{2n+1}^2}.$$

It is then natural to introduce the following map τ:

$$\tau(x,sy) = (x,sy)\circ[(z,s)\oplus(0,0)] = (x(z^{-1}), -\frac{s}{z^2}y(z^{-1}))$$

and to look at the quantity $(\bar{x}, s\bar{y}) = (x,sy)\ominus\tau(x,sy)$ in order to understand how close a solution over $\mathcal{M}_p$ is to having the above property of rational solutions. It will turn out that $(\bar{x}, s\bar{y})$ is a point of order 1 or 2 on $\mathcal{E}$. From this result, we will have enough information on x and y to conclude that they have to be rational (see subsection 8.4).

To see that the quantity $(\bar{x}, s\bar{y})$ has to be a point of order 1 or 2, we prove that

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

which implies that $\bar{x}$ and $z\bar{y}$ are invariant under the map $z\mapsto z^{-1}$. Note that $(\bar{x},\bar{y})$ is a solution of Equation (MD) over $\mathcal{M}_p^*$ (global meromorphic on $\mathbf{C}_p^* = \mathbf{C}_p - \{0\}$, such functions can have an essential singularity at 0). Also, Equation (MD) can be written:

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

Then our original problem has been reduced to studying the solutions of

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

over the field $\mathcal{M}_p^*$, which are invariant under the map $z \mapsto z^{-1}$. We show in subsection 8.2 that functions in $\mathcal{M}_p^*$ which are invariant under $z \mapsto z^{-1}$ are global meromorphic functions in the variable $w = z + z^{-1}$. Our problem is then reduced to finding the solutions of

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

over $\mathcal{M}_p$, where the independent variable is now w. Writing $t^2 = w + \delta$, one sees that we obtain an equation of the type of Equation (1), for which we have to find the solutions over $\mathcal{M}_p$. This problem is the object of section 7. It turns out that Equation (1) has only constant solutions over $\mathcal{M}_p$.

We have been informed by A. Escassut that the latter result had already been proved, in a more general context, by W. Berkovich (see the 1990's book [4, chap. 4, thm. 4.5.1]), and by himself and A. Boutabaa two years ago (in [5, cor. a, p. 3]) using p-adic Nevanlinna's theory. We decided to present our proof because we obtain at the same time some characterization of the solutions which are meromorphic on a disc. This characterization might provide a starting point for proving an analogue of the main theorem 1.2 for a field of non-global meromorphic functions, in the future.

6 Definitions - Notation - Basic results

The letters **Z**, **Q**, **R** and **C** will denote respectively the ring of integers, the fields of rational integers, real numbers and complex numbers. The letter T will be the indeterminate (for polynomials, powers series, ...). The letter z will always be a variable.

6.1 Formal series

If K is any field of characteristic zero, we will denote by $K[[T]]$ the ring of formal power series over K and by $K((T))$ the field of fractions of $K[[T]]$. We will denote by Id the identity in any formal power series ring, that is, the series T. We will denote by $\mathcal{V}\colon K((T)) \longrightarrow \mathbf{Z}$ the usual valuation on $K((T))$, that is, if $H \in K((T))$, we define $\mathcal{V}(H)$ by:

$$\mathcal{V}(H) = \max\{\, n \in \mathbf{Z} \mid T^{-n}H \in K[[T]]\,\},$$

if $H \neq 0$, and $\mathcal{V}(0) = -\infty$. If H is any element of $K((T))$, we will denote by H' the formal derivative of H. If A is a subset of K, and $h_0, \ldots, h_n$ are any elements of K, by

$$h_0 + h_1T + \cdots + h_nT^n + T^{n+1}A[[T]],$$

we will mean the set of power series having their $(n+1)$ first coefficients equal, respectively, to $h_0, \ldots, h_n$ and all the others coefficients elements of A.

6.2 Fields of p-adic numbers

We refer for the following basic facts to [25] or [42]. Let p be a fixed prime. For any non-zero integer n, denote by $\nu_p(n)$ the integer which satisfies

$$n = p^{\nu_p(n)}a,$$

such that p does not divide the integer a. We also define $\nu_p(0) = -\infty$. If $q = \frac{n}{m} \in \mathbf{Q}$, we define $\nu_p(q) = \nu_p(n) - \nu_p(m)$. We consider the absolute value on $\mathbf{Q}$ defined by:

$$|q|_p = p^{-\nu_p(q)}.$$

This absolute value is called the *p-adic absolute value.* It is multiplicative. Note that the p-adic absolute value of an integer is less than or equal to 1.

The field $\mathbf{Q}_p$ of *p-adic numbers* is the completion of $\mathbf{Q}$ with respect to the p-adic absolute value. A theorem of Ostrowski says that any non-trivial absolute value on $\mathbf{Q}$ is equivalent either to the usual absolute value or to a p-adic absolute value.

Let $\mathbf{C}_p$ denote the completion of the algebraic closure of the field $\mathbf{Q}_p$. The field $\mathbf{C}_p$ is algebraically closed, and therefore, it is considered as the p-adic analogue of the field $\mathbf{C}$ of complex numbers. We will call an element of $\mathbf{C}_p$ a *p-adic complex number.* Any p-adic complex number $z \neq 0$ can be written $z = p^ck$, where $|k|_p = 1$ and $|z|_p = p^{-c}$.

The p-adic absolute value is a non-Archimedean absolute value, that is, for any x and y in $\mathbf{C}_p$, we have

$$|x + y|_p \leq \max(|x|_p, |y|_p).$$

This inequality extends, by induction, to any finite sum (and even infinite, if we have convergence). One of the consequences of this inequality is that the field $\mathbf{C}_p$, as a topological space, is totally disconnected. This is a major difference from the complex case. In particular we have:

Lemma 6.1 *1. Any element of a disc is a center of this disc.*

2. Any disc (with its frontier or not), which is not a singleton, is both open and close.

3. The intersection of two discs is either empty or one of the two discs (that is, one of the discs is included in the other).

For any element α of $\mathbf{C}_p$ and any non-negative real r, we will denote by $\bar{D}(\alpha, r)$ the set $\{z \in \mathbf{C}_p \mid |z-\alpha|_p \leq r\}$, and, if r is strictly positive, by $D(\alpha, r)$ the set $\{z \in \mathbf{C}_p \mid |z-\alpha|_p < r\}$. The letter $\mathcal{D}$ will denote the *valuation ring of* $\mathbf{C}_p$, that is, $\mathcal{D} = \bar{D}(0,1)$.

6.3 Convergence of formal power series and formal infinite products

For the results below, we refer to [24] and [42, chap. 6]. A sequence of elements of $\mathbf{C}_p$ converges if and only if it is a Cauchy sequence. The following lemma indicates a major difference between $\mathbf{C}_p$ and $\mathbf{C}$:

Lemma 6.2 *A series $\sum_{n\geq 0} h_n$ converges if and only if the sequence h_n tends to zero as n goes to infinity.*

Lemma 6.3 *If $H = \sum_{n\geq 0} h_n$ is a convergent series, then the set $\{|h_n| \mid n \in \mathbf{N}\}$ has a maximum.*

The *radius of convergence* of a formal power series is defined as in the complex case. If $H = \sum_{n\geq 0} h_n T^n \in \mathbf{C}_p[[T]]$, then the radius of convergence of H is

$$\mathrm{RC(H)} = \frac{1}{\limsup_{\mathrm{n}\to\infty} \sqrt[n]{|h_n|_p}} = \mathrm{sup}\,\{\mathrm{r} \geq 0 \mid |\mathrm{h_n}|_\mathrm{p}\mathrm{r^n} \to 0\} \in \mathbf{R} \cup \infty.$$

A *convergent power series* is a power series with a non-zero radius of convergence. The problem of the convergence on the boundary of the disc of convergence is much simpler in $\mathbf{C}_p$ than in the complex case: if a power series converges at a point whose absolute value is r, then it converges at any point of the set $\{z \mid |z| = r\}$. A convergent power series defines a function on its disc of convergence in the usual way.

Here are some basic lemmas.

Lemma 6.4 *If H is a power series with all its coefficients in the valuation ring $\mathcal{D}$, then the radius of convergence of H is greater than or equal to* 1*.*

Lemma 6.5 *The formal sum and product of two convergent power series F and G is a convergent power series. If a convergent power series F is such that $\mathcal{V}(F) = 0$, then its formal inverse (for multiplication) is a convergent power series. If F and G are two convergent power series such that $\mathcal{V}(G) \geq 1$, then the formal composition $F \circ G$ is a convergent power series. The composition (under the above condition) is associative.*

Lemma 6.6 *Let K be either an extension of $\mathbf{Q}_p$ or an extension of* $\mathbf{R}$*. If H is any formal power series in $K[[T]]$, then the radii of convergence of H and H' are equal.*

Proof: See [42, chap.6, prop.3, p. 286]. ◇

Note that the disc of convergence of H' can be strictly included in the disc of convergence of H (see [42, chap. 6, p. 286] for an example).

In the following lemma, we resume some basic facts about products.

Lemma 6.7 *If $(h_n)_{n\geq 0}$ is a sequence in $\mathbf{C}_p$, converging to 1, then the sequence $\pi_N = \prod_{n=1}^N h_n$ converges. We write the limit as $\prod_{n\geq 1} h_n$. More generally, if $(h_n)_{n\geq 0}$ is a sequence of $\mathbf{C}_p$-valued functions defined on some set S, converging uniformly to 1 on S, then the sequence $\pi_N = \prod_{n=1}^N h_n$ converges uniformly to a function, denoted $\prod_{n\geq 1} h_n$.*

6.4 Inverse function theorem; a formal proof

If $F = \sum_{n\geq 1} a_n T^n \in K[[T]]$ is a convergent series, with $a_1 \neq 0$, then the formal inverse of F for composition is also a convergent series. We give here a formal proof of this inverse function theorem, supposing nevertheless that $\sup\{|a_n|\} < \infty$. One can find more information about the reciprocal of an analytic function in [24, chap. 27].

Lemma 6.8 *Let $f(T) = \sum_{n\geq 1} a_n T^n \in K[[T]]$ be a formal power series with coefficients in a field K of characteristic zero, and with $a_1 \neq 0$. Then there exists a unique formal power series $g(T) = \sum_{n\geq 1} b_n T^n$ such that $g(f(T)) = T$. Moreover, there are polynomials $P_n(X_1, \dots, X_n) \in \mathbf{Z}[X_1, \dots, X_n]$ of total degree $n-1$, which do not depend on f, such that the coefficients b_n can be written :*

$$b_n = \frac{P_n(a_1, \dots, a_n)}{a_1^{2n-1}}.$$

Proof: The existence and unicity of $g(T)$ is done in [29, chap. II, §6]. Let us prove the second part by induction on n. We have :

$$T = g(f(T)) = \sum_{n\geq 1} b_n \left(\sum_{k\geq 1} a_k T^k \right)^n = \sum_{n\geq 1} b_n (a_1 T + a_2 T^2 + a_3 T^3 + \cdots)^n.$$

We obtain the first relations :

$$\begin{aligned} 1 &= b_1 a_1, & b_1 &= \frac{1}{a_1} \\ 0 &= b_1 a_2 + b_2 a_1^2, & b_2 &= -\frac{a_2}{a_1^3} \\ 0 &= b_1 a_3 + 2 b_2 a_1 a_2 + b_3 a_1^3, & b_3 &= -\frac{a_3}{a_1^4} + 2\frac{a_2^2}{a_1^5}. \end{aligned}$$

Then the coefficients b_n satisfy the property for $n = 1, 2, 3$. Suppose now that $n \geq 2$ and the b_k, for $k = 1, \cdots, n-1$, all satisfy the property. We have :

$$\frac{a_n}{a_1} + \sum_{k=2}^{n-1} b_k P_{k,n}(a_1, \dots, a_{n-1}) + b_n a_1^n = 0 \tag{4}$$

where, for $k = 2, \dots, n-1$:

$$P_{k,n}(X_1, \dots, X_{n-1}) = \sum_{i_1+\cdots+i_k=n} X_{i_1} \dots X_{i_k},$$

where the indices $i_1, \dots, i_k$ are all ≥ 1. The total degree of the polynomial $P_{k,n}(X_1, \dots, X_{n-1})$ is k. If $d \in \mathbf{N}$ is such that X_1^d divides $P_{k,n}(X_1, \dots, X_{n-1})$, then $d \geq 2k - n$ (because if we take exactly d times the term X_1 in a monomial $X_{i_1} \dots X_{i_k}$, then we must choose $k - d$

quantities among the terms with index ≥ 2, $X_2, \ldots, X_{n-1}$; therefore the integer d satisfies $d + 2(k-d) \leq n$, and then $d \geq 2k - n$).

By the hypothesis of the induction, for $k < n$, we have:

$$b_k = \frac{P_k(a_1, \ldots, a_k)}{a_1^{2k-1}},$$

where $P_k(X_1, \ldots, X_k) \in \mathbf{Z}[X_1, \ldots, X_k]$ is of total degree $k-1$. Write d_k for the largest integer such that $X_1^{d_k}$ divides $P_{k,n}$ (then $d_k \geq 2k - n$). Write also:

$$\begin{aligned} Q_{k,n}(X_1, \ldots, X_{n-1}) &= \frac{P_k(X_1, \ldots, X_k)}{X_1^{2k-1}} P_{k,n}(X_1, \ldots, X_{n-1}) \\ &= \frac{1}{X_1^{2k-1-d_k}} \left(P_k \cdot \frac{P_{k,n}}{X_1^{d_k}} \right) \\ &= \frac{1}{X_1^{2k-1-d_k}} R_{k,n}, \end{aligned}$$

for some polynomial $R_{k,n} \in \mathbf{Z}[X_1, \ldots, X_{n-1}]$, so that Equation (4) becomes:

$$\frac{a_n}{a_1} + \sum_{k=2}^{n-1} Q_{k,n}(a_1, \ldots, a_{n-1}) + b_n a_1^n = 0, \tag{5}$$

which can be written also as:

$$b_n = \frac{1}{a_1^n} \left(-\frac{a_n}{a_1} - \sum_{k=2}^{n-1} \frac{1}{a_1^{2k-1-d_k}} R_{k,n}(a_1, \ldots, a_{n-1}) \right)$$

The power of X_1 in the denominator of $Q_{k,n}(X_1, \ldots, X_{n-1})$ is at most

$$2k - 1 - d_k \leq (2k-1) - (2k-n) = n - 1,$$

and the total degree of the polynomial

$$R_{k,n} = P_k \cdot \frac{P_{k,n}}{X_1^{d_k}}$$

is $(k-1) + k - d_k = 2k - 1 - d_k$. Let $S_{k,n}$, for $k = 2, \ldots, n-1$, be the polynomials such that

$$\frac{S_{k,n}}{X_1^{n-1}} = \frac{R_{k,n}}{X_1^{2k-1-d_k}}.$$

Then the degree of $S_{k,n}$ is $n-1$. We define P_n by

$$P_n(X_1, \ldots, X_n) = \frac{1}{X_1^{2n-1}} \left(-X_n X_1^{n-2} - \sum_{k=2}^{n-1} S_{k,n}(X_1, \ldots, X_{n-1}) \right).$$

Since the indeterminate X_n does not occur in the polynomials $S_{k,n}$, the polynomial P_n is of degree $n-1$. Obviously, we have

$$b_n = \frac{P_n(a_1, \ldots, a_n)}{a_1^{2n-1}}.$$

◇

Corollary 6.9 *With the notation as in Lemma 6.8, if* $|a_1|_p \geq 1$, *and* $f(T) \in a_1 + T\mathcal{D}[[T]]$, *then the formal inverse of* $f(T)$ *has all its coefficients in* $\mathcal{D}$.

Theorem 6.10 *Let*

$$f(T) = \sum_{n \geq 1} a_n T^n \in \mathbf{C}_p[[T]], \quad a_1 \neq 0,$$

be a formal power series with a positive radius of convergence and $\sup\{|a_n|\} < \infty$. *Then the formal inverse (for composition)* $g(T)$ *of* $f(T)$ *has also a positive radius of convergence.*

Proof: Let us write $g(T) = \sum_{n \geq 1} b_n T^n$. The set $\{|a_n|_p \mid n \geq 1\}$ has a maximum $|a_r|_p$. By Lemma 6.8, we have

$$\begin{aligned} |b_n|_p &= \frac{|P_n(a_1, \ldots, a_n)|_p}{|a_1|_p^{2n-1}} \\ &\leq \frac{1}{|a_1|_p^{2n-1}} |a_r|_p^{n-1}. \end{aligned}$$

Thus the sequence $\sqrt[n]{|b_n|_p}$ is bounded, which implies that

$$\limsup_{n \to \infty} \sqrt[n]{|b_n|_p} < \infty.$$

So the power series $g(T)$ has a positive radius of convergence. ◇

6.5 Meromorphic functions

Let us fix a non-empty disc D in $\mathbf{C}_p$, such that $D = D(\alpha, r)$ or $D = \bar{D}(\alpha, r)$ (r is allowed to be ∞). An *analytic function* f *on* D *(over* $\mathbf{C}_p$*)* will be a function defined on D which admits a power series expansion on D, i.e.:

$$\forall z \in D, \quad f(z) = \sum_{n \geq 0} a_n (z - \alpha)^n$$

for some formal power series

$$F_\alpha = \sum_{n \geq 0} a_n T^n \in \mathbf{C}_p[[T]]$$

which has a radius of convergence greater than or equal to r. The underlying power series F_α depends on α. However, the radius of convergence of F_α does not depend on α (this follows from Lemma 6.1, 1). Therefore, in the p-adic context, we do not have analytic continuation. We will call F_α the expansion of f around α, because it is unique (obviously).

An analytic function on all $\mathbf{C}_p$ will be called a *global analytic function.* We denote by $\mathcal{A}_p(D)$ the integral ring of analytic functions on D and by $\mathcal{A}_p$ the integral ring of global analytic functions. We denote by $\mathcal{M}_p(D)$ the fraction field of $\mathcal{A}_p(D)$ and by $\mathcal{M}_p$ the fraction field of $\mathcal{A}_p$. We will call an element of $\mathcal{M}_p(D)$ a *meromorphic function on* D (*over* $\mathbf{C}_p$) and an element of $\mathcal{M}_p$ a *global meromorphic function.*

From Lemma 6.5 we obtain:

Lemma 6.11 *1. Let* F *and* G *be two convergent power series, which are the expansions around a point* α *of* f *and* g *respectively. Let* H *denote the sum* $F+G$ *(resp. the product* FG*). Then* H *is the expansion around* α *of* $f+g$ *(resp.* fg*). Hence we can evaluate* h *in the usual way: if* $|z|_p < \min(\mathrm{RC(F)}, \mathrm{RC(G)})$, *then we have* $h(z) = f(z)+g(z)$ *(resp.* $h(z) = f(z)g(z)$*).*

2. *Under the same conditions as in 1, if we have $\mathcal{V}(G) \geq 1$, and if H denote the composition $F \circ G$, then H is the expansion around α of $f \circ g$. We can evaluate h in the usual way: if $|z|_p < \mathrm{RC(G)}$ and $|g(z)|_p < \mathrm{RC(F)}$, then we have $h(z) = f(g(z))$.*

3. *Under the same conditions as in 1, if we have $\mathcal{V}(F) \neq 0$, and if H denote the quotient $\frac{1}{F}$, then H is the expansion around α of $\frac{1}{f}$. We can evaluate h in the usual way: if $|z|_p < \mathrm{RC(F)}$ and $f(z) \neq 0$, then we have $h(z) = \frac{1}{f(z)}$.*

4. *Let $h = \frac{f}{g}$ be a meromorphic function, and let F and G be the expansions of respectively f and g around a point α. Then the expansion around α of h is given by the formal quotient $\frac{F}{G} \in \mathbf{C}_p((T))$.*

Note that the composition of two meromorphic functions is not necessarily a meromorphic function.

Corollary 6.12 1. *If $P \in \mathbf{C}_p[T]$ is such that $P(H) = 0$ for some power series $H \in \mathbf{C}_p[[T]]$ which is the expansion around a point of an analytic function h, then we have $P(h) = 0$*

2. *If $P \in \mathbf{C}_p(T)$ is such that $P(H) = 0$ for some Laurent series $H \in \mathbf{C}_p((T))$ which is the expansion around a point of a meromorphic function h, then we have $P(h) = 0$*

We will denote by Id the identity function of $\mathcal{A}_p(D)$, $\mathcal{A}_p$, $\mathcal{M}_p(D)$ or $\mathcal{M}_p$.

Definition 6.13 We will say that a meromorphic (resp. analytic) function f on D is *maximal* if there is no meromorphic (resp. analytic) function on a disc containing strictly D which is equal to f on D.

The order of a zero or a pole of a meromorphic function is well defined. See [42, chap.6, p. 305], for a proof of this fact and of the following assertions.

Lemma 6.14 *A meromorphic function has only finitely many zeros and poles in a disc of finite radius (with its frontier or not). A meromorphic function f has no accumulation of poles and, if $f \neq 0$, then f has no accumulation of zeros. Consequently, if two meromorphic functions take the same values on a set which has an accumulation point, then they are equal.*

Corollary 6.15 *Let f be a meromorphic function on a disc D. If, for any $z \in D$, we have $f'(z) = 0$, then f is a constant function.*

Note that if we ask the function f, instead of being meromorphic, to be differentiable everywhere (with its obvious meaning), then the corollary is not true (see [25, problem 263] for a counter example).

Corollary 6.16 *The image of a non-constant meromorphic function is a non-discrete set.*

Proof: If the function is global, it is clear. Then let f be a non-constant meromorphic function on a disc D of finite radius, and a an element in the image of f. Then, by Lemma 6.14, the set

$$\overset{-1}{f}(a) = \{z \in D \mid f(z) = a\}$$

is discrete. Therefore, if the image of f were discrete, then the disc D would be discrete, hence its radius would be zero. $\diamond$

From Lemma 6.7, we have:

Lemma 6.17 *Let $f \neq 0$ be a global analytic function on $\mathbf{C}_p$. Then f can be written as*

$$f(z) = Cz^m \prod \left(1 - \frac{z}{\rho}\right)^{\nu_\rho},$$

the product being taken over all the non-zero zeros ρ of f, and the integer ν_ρ being the multiplicity of f at ρ. The integer m is the multiplicity of f at 0.

A quotient of such infinite products is a meromorphic function. Moreover:

Lemma 6.18 *Let $D = \bar{D}(\alpha, r)$ be any disc in $\mathbf{C}_p$, with $0 < r \leq \infty$. A meromorphic function in $\mathcal{M}_p(D)$ can be written as the quotient of two analytic functions on $\mathcal{D}$ with no common zeros. This is not true for discs of the form $D(\alpha, r)$.*

Lemma 6.19 *1. A global analytic function either is a polynomial or has infinitely many zeros.*

2. A global analytic function is surjective.

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 it has a sequence of zeros (resp. poles) whose absolute value goes to infinity.

6.6 Elliptic curves

For all the definitions and basic results on elliptic curves, we refer to [28] and [46].

A non-singular plain projective curve $\mathcal{E}$ of genus 1 together with a point O of it has a natural structure of a commutative group, which makes $\mathcal{E}$ into an algebraic group with O the neutral element. We will denote the addition law on $\mathcal{E}$ by $\oplus$ (the symbol $\ominus$ will be used for the opposite). The pair $(\mathcal{E}, O)$ is called an *elliptic curve*. Let F be a field and $\mathbf{P}^2(F)$ the projective space over F. We write $\bar{F}$ for an algebraic closure of F. Such curves $\mathcal{E}$ can be written as the locus in $\mathbf{P}^2(\bar{F})$ of an equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

with $a_1, a_2, a_3, a_4, a_6 \in \bar{F}$. Note that the only point at infinity is $[0, 1, 0] \in \mathbf{P}^2(F)$. We will always choose this point for O, and we will write $\mathcal{E}$ instead of $(\mathcal{E}, O)$. Sometimes we will need to specify the field F, we will then write $\mathcal{E} = \mathcal{E}(F)$. Let K be a field. If the above coefficients a_i all lie in K, we say that *the curve is defined over K*. If K has characteristic $\neq 2, 3$ then, by an adequate change of variables, the above equation is equivalent to one of the form (see [46, chap. III, §1, p. 46]),

$$(\bigstar) \qquad Y^2Z = X^3 + aXZ^2 + bZ^3.$$

Writing $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, Equation ($\bigstar$) becomes

$$(\blacklozenge) \qquad y^2 = x^3 + \alpha x + \beta.$$

Every solution of Equation (★) in $\mathbf{P}^2(F)$, except for O, corresponds to a unique solution of Equation (♦) in F^2, and vice-versa. The set of solutions of Equation (♦) in F^2 is an *affine curve*, called *the affine part of the curve $\mathcal{E}$*. Write $\mathcal{E}_{\alpha,\beta}$ for the curve defined by Equation (♦). Let δ be any element of K. We will work with equations of the form

$$(1) \qquad y^2 = x^3 + \delta x^2 + x.$$

Equation (1) defines the affine part of an elliptic curve $\mathcal{E}_\delta$. Substituting x by $x - \frac{\delta}{3}$ in Equation (1), we obtain:

$$\begin{aligned} y^2 &= (x - \frac{\delta}{3})^3 + \delta(x - \frac{\delta}{3})^2 + x - \frac{\delta}{3} \\ &= (x^3 - \delta x^2 + \frac{\delta^2}{3}x - \frac{\delta^3}{27}) + \delta(x^2 - 2\frac{\delta}{3}x + \frac{\delta^2}{9}) + x - \frac{\delta}{3} \\ &= x^3 + (-\frac{\delta^2}{3} + 1)x + (2\frac{\delta^3}{27} - \frac{\delta}{3}). \end{aligned}$$

Thus, for $\alpha = -\frac{\delta^2}{3} + 1$ and $\beta = 2\frac{\delta^3}{27} - \frac{\delta}{3}$, the curve $\mathcal{E}_{\alpha,\beta}$ is isomorphic to the curve $\mathcal{E}_\delta$, through the isomorphism $(x, y) \mapsto (x - \frac{\delta}{3}, y)$. Write $\bar{K}$ for an algebraic closure of K.

Proposition 6.20 *Any elliptic curve defined over K is isomorphic (over $\bar{K}$) to a curve $\mathcal{E}_\delta$, for some $\delta \in \bar{K}$.*

Proof: To each class of isomorphisms of elliptic curves corresponds an element of $\bar{K}$ called *the modular invariant* or *the j-invariant.* In the bibliography, it is usually given for equations of the form

$$y^2 = 4x^3 - g_2 x - g_3,$$

where $g_2, g_3 \in K$. Write $\mathcal{E}_{g_2,g_3}$ the elliptic curve defined by such an equation. The modular invariant of $\mathcal{E}_{g_2,g_3}$ is

$$j(\mathcal{E}_{g_2,g_3}) = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}.$$

Every element of $\bar{K}$ is the modular invariant of some elliptic curve. The elliptic curve $\mathcal{E}_{g_2,g_3}$ is obviously isomorphic to the curve $\mathcal{E}_{\alpha,\beta}$, where $\alpha = -\frac{g_2}{\sqrt[3]{4}}$ and $\beta = -g_3$, through the isomorphism $(x, y) \mapsto (\frac{x}{\sqrt[3]{4}}, y)$. So we have

$$\begin{aligned} j(\mathcal{E}_\delta) = j(\mathcal{E}_{\alpha,\beta}) = j(\mathcal{E}_{g_2,g_3}) &= 1728\frac{g_2^3}{g_2^3 - 27g_3^2} \\ &= 1728\frac{4\alpha^3}{4\alpha^3 + 27\beta^2} \\ &= 1728\frac{4(-\frac{\delta^2}{3} + 1)^3}{4(-\frac{\delta^2}{3} + 1)^3 + 27(\frac{2\delta^3}{27} - \frac{\delta}{3})^2} \\ &= 1728\frac{4(-\delta^2 + 3)^3}{4(-\delta^2 + 3)^3 + (2\delta^3 - 9\delta)^2} \\ &= 1728\frac{4(-\delta^2 + 3)^3}{-27\delta^2 + 4 \cdot 27}. \end{aligned}$$

It is clear that the map

$$\begin{array}{rccc} j\colon & \bar{K} - \{\pm 2\} & \longrightarrow & \bar{K} \\ & \delta & \longmapsto & j(\mathcal{E}_\delta) \end{array}$$

is surjective. ◇

Let $(\mathcal{E}_1, O)$ and $(\mathcal{E}_2, O)$ be elliptic curves. An *isogeny* between $(\mathcal{E}_1, O)$ and $(\mathcal{E}_2, O)$ is a morphism of curves $\mathcal{E}_1 \longrightarrow \mathcal{E}_2$ which sends O to O. An isogeny is a morphism of algebraic groups. The set of isogenies from a curve $\mathcal{E}$ to itself is called the *ring of endomorphisms of* $\mathcal{E}$, and is denoted by $\mathrm{End}\,(\mathcal{E})$. If K has characteristic zero, it is a free $\mathbf{Z}$-module of rank 1 (in which case we say that *the curve has no complex multiplication*) or 2 (in which case we say that *the curve has complex multiplication*).

We will give now the addition formulas for the curves $\mathcal{E}_\delta$. We refer for this to [46, chap. III, p. 58]. For Equation (1), we obtain :

Group Law Algorithm :

Let $P_3 = P_1 \oplus P_2$, with, for $i = 1, 2$, $P_i = (x_i, y_i) \in \mathcal{E}_\delta$.
(a) The opposite is given by

$$\ominus P_1 = (x_1, -y_1).$$

If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 \oplus P_2 = O$.
Otherwise $P_3 = (x_3, y_3)$ where
(b) if $x_1 \neq x_2$, then

$$\begin{aligned} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - \delta - x_1 - x_2, \\ y_3 &= -\frac{y_2 - y_1}{x_2 - x_1} x_3 - \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1}, \end{aligned}$$

which is equivalent to :

$$\begin{aligned} x_3 &= \frac{(y_1 x_2 - x_1 y_2)^2}{x_1 x_2 (x_2 - x_1)^2}, \\ y_3 &= -\frac{(y_2 - y_1)(y_1 x_2 - x_1 y_2)^2}{x_1 x_2 (x_2 - x_1)^3} - \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1}, \end{aligned}$$

(c) if $x_1 = x_2$ and $y_1 = y_2 \neq 0$, we have the *duplication formula* :

$$\begin{aligned} x_3 &= \frac{(x_1^2 - 1)^2}{4y_1^2} = \frac{(x_1^2 - 1)^2}{4(x^3 + \delta x^2 + x)} \\ y_3 &= -\frac{(3x_1^2 + 2\delta x_1 + 1)(x_1^2 - 1)^2 - 4y_1^2(x_1^3 - x)}{8y_1^3}. \end{aligned}$$

(d) if $y_1 = 0$, then x_1 is a root ξ of the polynomial $T^3 + \delta T^2 + T$. The points $(\xi, 0)$ are of order 2. ◇

In our context, the field K will be either the field $\mathbf{C}_p$ of p-adic complex numbers (see subsection 6.2), or the field $\mathbf{C}_p(z)$ of rational functions over $\mathbf{C}_p$. The field F will be the field $\mathcal{M}_p$ of p-adic global meromorphic functions.

7 Meromorphic parametrizations of elliptic curves over $\mathbf{C}_p$

In this section, K will denote any field of characteristic zero and $K^\star = K - \{0\}$. We will indicate if K is needed to be algebraically closed. Let δ be any constant in K such that $\delta^2 \neq 4$. Then the equation

$$y^2 = x^3 + \delta x^2 + x \tag{1}$$

defines an elliptic curve. We will call $\mathcal{E}$ this elliptic curve. The aim of this section is to prove the following theorem :

Theorem 7.1 *[Berkovich] There is no global p-adic meromorphic parametrization of elliptic curves over $\mathbf{C}_p$.*

In other words, Equation (1) cannot be satisfied by non-constant functions in $\mathcal{M}_p$. This theorem is a special case of a more general theorem by W. Berkovich (see [4, chap. 4 , Thm. 4.5.1]). It has also been proved using p-adic Nevanlinna's theory (see [5, Cor. a, p. 3]).

We will call a *local meromorphic solution* of Equation (1) any pair $(x, y) \in \mathcal{M}_p(D)^2$ which satisfies Equation (1), where D is any disc with positive radius.

If X and Y are elements of $K((T))$ such that (X, Y) satisfies Equation (1), we will call (X, Y) *a Laurent solution (of (1) over K).* If moreover, for some constant $\eta \in K$, we have $X' = \eta Y$, we will call (X, Y) *an η-Weierstrass Laurent solution (of (1) over K).* Note that (X, Y) is an η-Weierstrass Laurent solution if and only if $(X, \frac{1}{\eta}X')$ is a Laurent solution. Let $H \in K((T))$. We will call $(H, \frac{1}{\eta}H')$ *an η-Weierstrass strictly Laurent solution (of (1) over K)* if $\mathcal{V}(H) < 0$ and *an η-Weierstrass power series solution (of* (1) *over K)* if $\mathcal{V}(H) \geq 0$ (where $\mathcal{V}$ is the usual valuation, see subsection 6.1). Analogously, we will call the power series H either *an η-Weierstrass Laurent series (for $\mathcal{E}$ over K)*, or *an η-Weierstrass strictly Laurent series (for $\mathcal{E}$ over K)* or *an η-Weierstrass power series (for $\mathcal{E}$ over K).* If $\eta = 1$, we will not mention η (so, for example, a *Weierstrass power series solution* is a 1-Weierstrass power series solution).

In subsection 7.1, we will prove the existence, for any $\eta \in K^\star$, of η-Weierstrass Laurent solutions (for any field K of characteristic zero). Among these solutions, for each η, two are of a particular interest. We will call these two specific solutions *the η-Weierstrass power series* and *the η-Weierstrass Laurent series* (of $\mathcal{E}$). This is justified by the fact that, for $\eta = 1$, the Weierstrass Laurent series is just the Laurent expansion of the usual Weierstrass function over $\mathbf{C}$. Up to this point, we will not be able to prove any convergence result, by lack of information on the coefficients of the Weierstrass series.

In subsection 7.2, we will deal with convergence of power series, in order to prove that some local meromorphic solutions exist. First, we will consider a particular formal solution which we will denote by (Γ, Θ). A particular property of this solution is that the coefficients of the formal series Γ and Θ lie in the algebraic extension $\mathbf{Z}[\delta]$ of the integers. This property, with the fact that we can bound the degree in δ of the coefficients of Γ and Θ, will give us a first result of convergence. Then we will consider a particular example of Weierstrass power series of an elliptic curve for which we know how to compute effectively the radius of convergence. One can see that this last result would have been sufficient to obtain the main theorem 1.2, by working only with this particular elliptic curve.

In subsection 7.3, we will prove some formal results of factorization (for the composition law) of Laurent solutions by the Weierstrass Laurent solution and by the Weierstrass power series solution.

In subsection 7.4, we will prove, by using the factorization results and the existence of a local meromorphic solution, that any Weierstrass power series has a positive (but finite) radius of convergence.

In subsection 7.5, we will finish the proof of Theorem 7.1.

7.1 Formal Weierstrass parametrizations

The field K is of characteristic zero, and contains δ and η.

Lemma 7.2 *Let $H = \sum_{n \geq 0} h_n T^n$ be an element of $K[[T]]$. The power series H is an η-Weierstrass power series for $\mathcal{E}$ if and only if its coefficients satisfy the following recursive relation :*

$$\begin{aligned} h_1^2 &= \eta^2(h_0^3 + \delta h_0^2 + h_0), \\ h_2 &= \frac{\eta^2}{4}(3h_0^2 + 2\delta h_0 + 1), \\ h_{n+2} &= \frac{\eta^2}{2(n+2)(n+1)} \left(3 \sum_{i=0}^{n} h_i h_{n-i} + 2\delta h_n \right), \quad \textit{if} \quad n \geq 1. \end{aligned}$$

Proof: We get the relation between h_1 and h_0 just by equating terms of degree 0 in

$$(\bigstar) \qquad (\tfrac{1}{\eta}H')^2 = H^3 + \delta H^2 + H,$$

where $H' = \sum_{n \geq 0} (n+1)h_{n+1}T^n$. Now by differentiating formally the sides of Equation ($\bigstar$), we obtain :

$$\frac{2}{\eta^2}H'' = 3H^2 + 2\delta H + 1,$$

with $H'' = \sum_{n \geq 0} (n+2)(n+1)h_{n+2}T^n$. Then our equality becomes :

$$\begin{aligned} \frac{2}{\eta^2} \sum_{n \geq 0} (n+2)(n+1)h_{n+2}T^n &= 3 \left(\sum_{n \geq 0} h_n T^n \right)^2 + 2\delta \sum_{n \geq 0} h_n T^n + 1 \\ &= 3 \sum_{n \geq 0} \left(\sum_{i=0}^{n} h_i h_{n-i} \right) T^n + 2\delta \sum_{n \geq 0} h_n T^n + 1 \end{aligned}$$

which gives us, by identification of terms of the same degree, h_2 for $n = 0$, and for $n \geq 1$, h_{n+2} in terms of $h_0, h_1, \ldots, h_n$. ◇

It follows from Lemma 7.2 that :

Corollary 7.3 *For each $\eta \in K^\star$:*

1. *There exists at most one η-Weierstrass power series H for $\mathcal{E}$ over K with constant term equal to a root of the polynomial $X^3 + \delta X^2 + X$; exactly one if K contains the non-zero roots of this polynomial.*

2. *There exists a unique η-Weierstrass power series H for $\mathcal{E}$ over K such that $\mathcal{V}(H) > 0$, and then $\mathcal{V}(H) = 2$. We will write this particular solution Q_η (or Q if $\eta = 1$). The coefficients of Q_η lie in the polynomial ring $\mathbf{Q}[\delta, \eta] \subset K$.*

3. *There exist at most two η-Weierstrass power series over K with constant term not a root of $X^3+\delta X^2+X$ (exactly two if K is algebraically closed). In any case, whenever the constant term h_0 of H has been fixed, all coefficients of H lie in the polynomial ring* $\mathbf{Q}[\delta, \eta, h_0, \sqrt{h_0^3+\delta h_0^2+h_0}]$.

4. *We have* $Q_\eta = Q \circ (\eta \mathrm{Id})$.

Proof: Statements 1, 2 and 3 are obvious. The last assertion is obtained in the following way: Write $h_n(\eta)$ the coefficients of Q_η. It is then obvious that $h_2(\eta) = \eta^2 h_2(1)$ and then, by induction, that $h_n(\eta) = \eta^n h_n(1)$. ◇

Remark 7.4 If H is an η-Weierstrass Laurent series for $\mathcal{E}$ over K, then $\frac{1}{H}$ is also an η-Weierstrass Laurent series for $\mathcal{E}$ over K.

Corollary 7.5 *For each $\eta \in K^\star$, there exists a unique η-Weierstrass strictly Laurent series for $\mathcal{E}$ over K.*

Proof: The existence and unicity follow by combining Remark 7.4 and Corollary 7.3. The Laurent series is $\frac{1}{Q_\eta}$. ◇

We will denote by P_η (resp. P) the formal inverse of Q_η (resp. Q). Note that, by Corollary 7.3 (4), we have $P_\eta = P \circ (\eta \mathrm{Id})$.

Lemma 7.6 *The coefficients of the series P_η lie in* $\mathbf{Q}[\delta, \eta]$.

Proof: We have

$$\begin{aligned}\frac{1}{Q_\eta} &= \frac{1}{\sum_{n\geq 2} h_n T^n} \\ &= \frac{1}{h_2 T^2} \frac{1}{1+\sum_{n\geq 3} \frac{h_n}{h_2} T^{n-2}} \\ &= \frac{1}{h_2 T^2}\left[1 - \sum_{n\geq 3} \frac{h_n}{h_2} T^{n-2} + \cdots\right].\end{aligned}$$

We know from Lemma 7.2 that $h_2 = \frac{\eta^2}{4}$, and that the other coefficients h_n of Q are polynomials in δ and η, divisible by η^2. Then the coefficients of P_η are finite sums of polynomials in the variables δ and η. ◇

Definition 7.7 We will call Q_η *the η-Weierstrass power series of $\mathcal{E}$* and P_η *the η-Weierstrass Laurent series of $\mathcal{E}$*. If $\eta = 1$, we will call Q *the Weierstrass power series of $\mathcal{E}$* and P *the Weierstrass Laurent series of $\mathcal{E}$*.

Remark 7.8 By Corollary 7.3, we have, for each $\eta \in K^\star$,

$$\mathcal{V}(P_\eta) = -\mathcal{V}(Q_\eta) = -2.$$

Moreover, the Weierstrass power series Q_η is even. This follows from Lemma 7.2: if $h_0 = 0$, then $h_1 = 0$; then, by induction, looking at the expression of h_{n+2}, we can see that h_{n+2} must be zero if n is odd. Consequently, P_η is also even, and the derivatives Q'_η and P'_η must be odd.

Lemma 7.9 *Let n be a non-zero integer. Write*

$$(S,T)=n(P,P'),$$

where addition is meant on the elliptic curve $\mathcal{E}$. Then the series S is the n-Weierstrass Laurent series. In other words, we have

$$n(P,P')=(P,P')\circ(n\mathrm{Id}).$$

Proof: We will prove by induction that if $(S,T)=n(P,P')$, then we have:

$$(\mathbf{P}_n) \qquad S'=nT \text{ and } \mathcal{V}(S)=-2.$$

Therefore, since (S,T) satisfies Equation (1), by applying Corollary 7.5, we will have proved that S is the n-Weierstrass Laurent series.

First, let us prove that the property $(\mathbf{P}_n)$ is true for $n=2$; so we assume that $(S,T)=(P,P')\oplus(P,P')=2(P,P')$. The relation between S, T, P and P' is given by the duplication formula (algebraically) on the elliptic curve, that is (see subsection 6.6):

$$\begin{aligned}S&=\frac{(P^2-1)^2}{4P'^2}\\ T&=-\frac{(3P^2+2\delta P+1)(P^2-1)^2-4P'^2(P^3-P)}{8P'^3}.\end{aligned}$$

Therefore, we have:

$$\begin{aligned}S'=2T &\Leftrightarrow \frac{4P'^3P(P^2-1)-2P''P'(P^2-1)^2}{4P'^4}=-\frac{(3P^2+2\delta P+1)(P^2-1)^2-4P'^2(P^3-P)}{4P'^3}\\ &\Leftrightarrow 4P'^3(P^3-P)-2P''P'(P^2-1)^2=-(3P^2+2\delta P+1)(P^2-1)^2P'+4P'^3(P^3-P)\\ &\Leftrightarrow 2P''P'(P^2-1)^2=(3P^2+2\delta P+1)(P^2-1)^2P'\\ &\Leftrightarrow 2P''P'=(3P^2+2\delta P+1)P'\\ &\Leftrightarrow (P')^2=P^3+\delta P^2+P.\end{aligned}$$

The last equality says that (P,P') satisfies Equation (1). Moreover we have

$$\begin{aligned}\mathcal{V}(S)&=\mathcal{V}\left(\frac{(P^2-1)^2}{4P'^2}\right)\\ &=2\mathcal{V}(P^2-1)-2\mathcal{V}(P')\\ &=4\mathcal{V}(P)-2\mathcal{V}(P')\\ &=-8+6=-2.\end{aligned}$$

Therefore, the property $(\mathbf{P}_2)$ is true. It implies, by Corollary 7.5, that $S=P_2$.

Let us suppose that the property $(\mathbf{P}_k)$ is true for $k\leq n$. If we write

$$(U,V)=(n+1)(P,P')=n(P,P')\oplus(P,P')=(S,T)\oplus(P,P'),$$

we have to prove that $U'=(n+1)V$ and that $\mathcal{V}(U)=-2$. By induction hypothesis, we have $S'=nT$ and $\mathcal{V}(S)=-2$, which implies that $S=P_n$ (by Corollary 7.5). Write $A=(TP-SP')$. The addition formula gives:

$$\begin{aligned}U&=\frac{(TP-SP')^2}{SP(P-S)^2}=\frac{A^2}{SP(P-S)^2}\\ V&=-\frac{(P'-T)(TP-SP')^2}{SP(P-S)^3}-\frac{TP-SP'}{P-S}=-\frac{(P'-T)A^2}{SP(P-S)^3}-\frac{A}{P-S}.\end{aligned}$$

We have

$$U' = \frac{2AA'SP(P-S)^2 - A^2[(S'P+SP')(P-S)^2 + 2SP(P-S)(P'-S')]}{(SP)^2(P-S)^4}.$$

Multiplying U' and V by

$$\frac{(SP)^2(P-S)^3}{A},$$

we obtain (calling α and β the two new quantities)

$$\begin{aligned}
\alpha &= \frac{(SP)^2(P-S)^3}{A}U' = 2A'SP(P-S) - A[(S'P+SP')(P-S) + 2SP(P'-S')] \\
\beta &= \frac{(SP)^2(P-S)^3}{A}V = -SP(P'-T)A - (SP)^2(P-S)^2.
\end{aligned}$$

We have to prove that $\alpha = (n+1)\beta$. Defining B and C such that $\alpha = B - C$, we have, on the one hand,

$$\begin{aligned}
B &= 2A'SP(P-S) \\
&= 2[T'P + TP' - S'P' - SP'']SP(P-S) \\
&= 2[T'P + TP' - nTP' - SP'']SP(P-S) \\
&= 2[ST'P^2 + (1-n)STPP' - S^2PP''](P-S)
\end{aligned}$$

and

$$\begin{aligned}
C &= A[(S'P+SP')(P-S) + 2SP(P'-S')] \\
&= A[S'P^2 - S'PS + SP'P - S^2P' + 2SPP' - 2SPS'] \\
&= A[S'P^2 - 3SS'P + 3SPP' - S^2P'] \\
&= (TP - SP')[nTP^2 - 3nSTP + 3SPP' - S^2P'] \\
&= nT^2P^3 - 3nST^2P^2 + 3STP^2P' - S^2TPP' - nSTP^2P' + 3nS^2TPP' - 3S^2PP'^2 + S^3P'^2 \\
&= nT^2P^3 - 3nST^2P^2 + (3-n)STP^2P' + (3n-1)S^2TPP' - 3S^2PP'^2 + S^3P'^2.
\end{aligned}$$

On the other hand, we have

$$\begin{aligned}
\beta &= -SP(P'-T)A - (SP)^2(P-S)^2 \\
&= (-SPP' + SPT)(TP - SP') - (SP)^2(P^2 - 2PS + S^2) \\
&= (-STP^2P' + S^2PP'^2 + ST^2P^2 - S^2TPP') - (S^2P^4 - 2S^3P^3 + S^4P^2).
\end{aligned}$$

The quantity S^2TPP' occurs in B with a coefficient $2(n-1)$, in C with a coefficient $3n-1$, then it occurs in α with a coefficient $2(n-1)-(3n-1) = -n-1$; also it occurs in $(n+1)\beta$ with the same coefficient, then it cancels. The quantity STP^2P' occurs in B with a coefficient $2(1-n)$, in C with a coefficient $3-n$, then it occurs in α with a coefficient $2(1-n)-(3-n) = -1-n$; it occurs in $(n+1)\beta$ with the same coefficient, then again, it cancels. Write B' and C', respectively, for B and C, in which we have cancelled these two quantities; write $\mu = B' - C'$; Write also ν for β in which we have also cancelled the two quantities S^2TPP' and STP^2P'. More precisely, we have

$$\begin{aligned}
B' &= 2[ST'P^2 - S^2PP''](P-S), \\
C' &= nT^2P^3 - 3nST^2P^2 - 3S^2PP'^2 + S^3P'^2, \\
\nu &= (S^2PP'^2 + ST^2P^2) - (S^2P^4 - 2S^3P^3 + S^4P^2)
\end{aligned}$$

and we must prove that $\mu := B' - C' = (n+1)\nu$. Since (S,T) and (P,P') satisfy Equation (1), we can replace everywhere T^2 by $S^3 + \delta S^2 + S$ and P'^2 by $P^3 + \delta P^2 + P$. Then B', C'

and ν are all multiple of SP. We define $B'' = \frac{B'}{SP}$, $C'' = \frac{C'}{SP}$, $\mu' = \frac{\mu}{SP}$ and $\nu' = \frac{\nu}{SP}$. We have now

$$\begin{aligned}
B'' &= 2[T'P - SP''](P - S), \\
C'' &= n(S^2 + \delta S + 1)P^2 - 3nT^2P - 3SP'^2 + S^2(P^2 + \delta P + 1), \\
\nu' &= (SP'^2 + T^2P) - (SP^3 - 2S^2P^2 + S^3P),
\end{aligned}$$

and we have to prove that $\mu' := B'' - C'' = (n+1)\nu'$. By differentiating the sides of the equality $T^2 = S^3 + \delta S^2 + S$, we obtain

$$2T'T = 3S'S^2 + 2\delta S'S + S' = S'(3S^2 + 2\delta S + 1) = nT(3S^2 + 2\delta S + 1),$$

and then we have

$$2T' = n(3S^2 + 2\delta S + 1).$$

We obtain in the same way

$$2P'' = 3P^2 + 2\delta P + 1.$$

Then B'' becomes

$$\begin{aligned}
B'' &= 2[T'P - SP''](P - S) \\
&= [n(3S^2 + 2\delta S + 1)P - S(3P^2 + 2\delta P + 1)](P - S) \\
&= [3nS^2P + 2n\delta SP + nP - 3SP^2 - 2\delta SP - S](P - S) \\
&= [3nS^2P + (2n-2)\delta SP + nP - 3SP^2 - S](P - S) \\
&= (3n+3)S^2P^2 + (2n-2)\delta SP^2 + nP^2 - 3SP^3 - (n+1)SP - 3nS^3P - (2n-2)\delta S^2P + S^2 \\
&= -3nS^3P + (3n+3)S^2P^2 - (2n-2)\delta S^2P + S^2 - 3SP^3 + (2n-2)\delta SP^2 - (n+1)SP + nP^2.
\end{aligned}$$

By replacing T^2 and P'^2 in C'', it becomes

$$\begin{aligned}
C'' &= n(S^2 + \delta S + 1)P^2 - 3n(S^3 + \delta S^2 + S)P - 3S(P^3 + \delta P^2 + P) + S^2(P^2 + \delta P + 1) \\
&= -3nS^3P + (n+1)S^2P^2 + (-3n+1)\delta S^2P + S^2 - 3SP^3 + (n-3)\delta SP^2 - (3n+3)SP + nP^2.
\end{aligned}$$

Then we have

$$\begin{aligned}
\mu' &= B'' - C'' \\
&= (2n+2)S^2P^2 + (n+1)\delta S^2P + (n+1)\delta SP^2 + (2n+2)SP.
\end{aligned}$$

Finally, ν' becomes

$$\begin{aligned}
\nu' &= S(P^3 + \delta P^2 + P) + (S^3 + \delta S^2 + S)P - SP^3 + 2S^2P^2 - S^3P \\
&= SP^3 + \delta SP^2 + SP + S^3P + \delta S^2P + SP - SP^3 + 2S^2P^2 - S^3P \\
&= \delta SP^2 + 2SP + \delta S^2P + 2S^2P^2 \\
&= 2S^2P^2 + \delta S^2P + \delta SP^2 + 2SP.
\end{aligned}$$

So we have $\mu' = (n+1)\nu'$ and therefore $U' = (n+1)V$.

We still have to prove that $\mathcal{V}(U) = -2$. Note that, by the induction hypothesis, we know that $S = P_n$. We have

$$\begin{aligned}
\mathcal{V}(U) &= \mathcal{V}\left(\frac{(TP - SP')^2}{SP(P-S)^2}\right) \\
&= 2\mathcal{V}(TP - SP') - \mathcal{V}(SP) - 2\mathcal{V}(P - S) \\
&= 2\mathcal{V}(\frac{1}{n}S'P - SP') - \mathcal{V}(SP) - 2\mathcal{V}(P - S) \\
&= 2\mathcal{V}(\frac{1}{n}P_n'P - P_nP') + 4 - 2\mathcal{V}(P - P_n).
\end{aligned}$$

Write α the coefficient of $\frac{1}{T^2}$ in P. Then the coefficient of $\frac{1}{T^3}$ in P' is -2α. Moreover we have

$$P'_n = (P \circ (n\mathrm{Id}))' = \mathrm{nP}' \circ (\mathrm{nId}),$$

and then

$$\frac{1}{n} P'_n P = P' \circ (n\mathrm{Id})\mathrm{P}.$$

Hence, the coefficient of $\frac{1}{T^5}$ in the latter is $\frac{-2\alpha}{n^3}\alpha$, while in $P_n P'$, the coefficient of $\frac{1}{T^5}$ is: $\frac{\alpha}{n^2}(-2\alpha)$. We obtain

$$\mathcal{V}(\frac{1}{n} P'_n P - P_n P') = -5.$$

The coefficient of $\frac{1}{T^2}$ in $P - P_n$ is: $\alpha - \frac{\alpha}{n^2} \neq 0$. Then we have $\mathcal{V}(P - P_n) = -2$. Finally, we obtain $\mathcal{V}(U) = -2$. ◇

Note: The following is an alternative proof of Lemma 7.9: Let $n \in \mathrm{End}\,(\mathcal{E}) - \{0\}$. Embed $\mathbf{C}_p$ into $\mathbf{C}$, as fields (it is well known that this can be done). Since δ has been chosen not equal to 2 in $\mathbf{C}_p$, δ cannot be mapped on 2, therefore the equation $s^2 = z^3 + \delta z^2 + z$ defines an elliptic curve over $\mathbf{C}$. Let $n \otimes P$ be defined by $(n \otimes P, n \otimes P') = n(P, P')$. The power series (around $z = 0$) $n \otimes P$ and $n \otimes P'$ are rational functions in P and P' over $\mathbf{C}_p$ and over $\mathbf{C}$. They define the usual meromorphic Weierstrass functions of $\mathcal{E}$, considered as a curve over $\mathbf{C}$. It is known that the functions $(P, P') \circ (nId)$ and $n(P, P')$, as functions over $\mathbf{C}$, coincide. Therefore the pairs of power series $(P, P') \circ (nId)$ and $(n \otimes P, n \otimes P')$ coincide. Therefore they coincide also over $\mathbf{C}_p$.

7.2 Existence of local meromorphic parametrizations

In the first part of this subsection, we will study a solution of Equation (1) for which we can find a lower-bound for the radius of convergence. The advantage is that it will work for any δ. These specific solutions appear in [46, chap. IV, §1, pp. 110-114] in the study of the formal law of an elliptic curve. In the second part, we will compute precisely the radius of convergence of a Weierstrass power series (for a specific elliptic curve).

First, we study the solutions (X, Y) of Equation (1) such that $X = TY$. We have to solve

$$\left(\frac{X}{T}\right)^2 = X^3 + \delta X^2 + X,$$

that is,

$$(\clubsuit) \qquad X = T^2(X^2 + \delta X + 1).$$

Let K be a field of characteristic zero, which contains δ.

Lemma 7.10 *Let $X = \sum_{n\geq 0} h_n T^n$ be an element of $K[[T]]$. The power series X satisfies Equation ($\clubsuit$) if and only if its coefficients satisfy the following recursive relation:*

$$h_0 = h_1 = 0,\ h_2 = 1, \quad \textit{and}$$
$$h_{n+2} = \sum_{i=0}^{n} h_i h_{n-i} + \delta h_n, \quad \textit{if} \quad n \geq 1.$$

Proof: We proceed as in Lemma 7.2. Equation (♣) is equivalent to

$$T^2X^2 + (\delta T^2 - 1)X + T^2 = 0,$$

which is equivalent to

$$T^2 \sum_{n\geq 0} \left(\sum_{i=0}^{n} h_i h_{n-i} \right) T^n + (\delta T^2 - 1) \sum_{n\geq 0} h_n T^n + T^2 = 0,$$

and we obtain the relations we want by equating terms of the same degree. ◇

Corollary 7.11 *1. There exists a unique power series solution (X, Y) of Equation (1) which satisfies $X = TY$. We will write this solution as (Γ, Θ).*

2. We have $\mathcal{V}(\Gamma) = 2$ and $\mathcal{V}(\Theta) = 1$.

3. The coefficients of Γ lie in $\mathbf{Z}[\delta]$. Moreover, if we write $\Gamma = \sum_{n\geq 0} h_n T^n$, then $h_{2n+1} = 0$ for any positive integer n, and h_{2n} is a polynomial of degree $n - 1$ in δ, for $n \geq 1$.

4. The power series Γ is not a Weierstrass power series.

Proof: Assertions 1 and 2 follow from Lemma 7.10. We prove Assertion 3 by induction on n. The fact that the odd coefficients are all zero is obvious by induction. Let us compute the two non-zero terms: we have $h_2 = 1$ and $h_4 = \delta h_2 = \delta$. Suppose n is even and h_i has degree $\frac{i}{2} - 1$ for $i = 2, \ldots, n$, and i even. Let us prove that h_{n+2} has degree $\frac{n}{2}$. If i is odd, then $h_i h_{n-i} = 0$. If i is even, then $h_i h_{n-i}$ has degree

$$\left(\frac{i}{2} - 1\right) + \left(\frac{n-i}{2} - 1\right) = \frac{n}{2} - 2.$$

The degree of δh_n is

$$1 + \left(\frac{n}{2} - 1\right) = \frac{n}{2}.$$

Therefore, the degree of h_{n+2} is $\frac{n}{2}$.

For the last assertion, if Γ were a Weierstrass power series, then we would have $\frac{\Gamma}{T} = \Gamma'$. We see by looking at the coefficient h_2 that this is not the case. ◇

Note that, for certain value of δ, the power series Γ may be a polynomial (this would happen if there exists an N such that for all $n \geq N$, the polynomials h_{2n} have a common root). We will know at the end of Section 7.5 that this is not possible, since we will have proved that there are no global parametrization of elliptic curves.

If δ is in the valuation ring $\mathcal{D}$ of $\mathbf{C}_p$, then all the coefficients of Γ will be in $\mathcal{D}$ (because a sum of terms of absolute value ≤ 1 has absolute value ≤ 1). Therefore, by Lemma 6.4, the power series Γ converges on a disc of radius ≥ 1. If δ has absolute value strictly greater than 1, we need the following lemma.

Lemma 7.12 *Let α be any non-zero element of $\mathbf{C}_p$ whose absolute value is ≥ 1, and let $H = \sum_{n\geq 0} h_n T^n$ be a power series with coefficients in $\mathbf{Z}[\alpha]$. If, for any n, the degree of the polynomial h_n in α is less than or equal to $an + b$, where a and b are some fixed constants in $\mathbf{C}_p$, then the radius of convergence of H is greater than or equal to $\frac{1}{|\alpha|_p^a}$.*

Proof: Since h_n has integer coefficients, and $|\alpha|_p \geq 1$, we have

$$|h_n|_p \leq \max_{i=0}^{an+b} |\alpha|_p^i = |\alpha|_p^{an+b}.$$

Therefore we have

$$\sqrt[n]{|h_n|_p} \leq \sqrt[n]{|\alpha|_p^{an+b}} = |\alpha|_p^{a+\frac{b}{n}},$$

which tends to $|\alpha|_p^a$ as n goes to infinity. Finally, we obtain:

$$\frac{1}{\limsup \sqrt[n]{|h_n|_p}} \geq \frac{1}{|\alpha|_p^a}.$$

$\diamond$

Corollary 7.13 *For any $\delta \in \mathbf{C}_p$, the radius of convergence of the power series Γ, hence also of Θ, is positive. If $|\delta|_p \geq 1$, then the radius of convergence of Γ is greater than or equal to $\frac{1}{\sqrt{|\delta|_p}}$. Otherwise, it is greater than or equal to 1.*

Therefore Γ and Θ define some local meromorphic functions γ and θ and the couple (γ, θ) is then a local meromorphic solution of Equation (1). The existence of this local solution does not imply obviously the existence of a Weierstrass local solution (that is, a local meromorphic solution (x, y) satisfying $x' = y$). We will prove later that, actually, it implies that any Weierstrass power series has a positive radius of convergence. We will give an example now to which we will find a Weierstrass power series solution and we will compute its radius of convergence.

Lemma 7.14 *Let K be any algebraically closed field of characteristic zero and let $\lambda \in K - \{0\}$. The following recursive relation*

$$a_{n+2} = \frac{3\lambda}{2(n+1)(n+2)} \sum_{i=0}^{n} a_i a_{n-i}, \quad \text{n} \geq 0$$

is satisfied by the sequences

$$\begin{aligned} a_n &= \frac{n+1}{\lambda 2^n}, & a_0 = 1,\ a_1 = \frac{1}{\lambda} \\ \textit{and} \quad a_n &= \frac{n+1}{2^n} \lambda^{\frac{n}{2}}, & a_0 = 1,\ a_1 = \lambda^{\frac{1}{2}} \end{aligned}$$

Proof: Let us show that this is true for $\lambda = 1$. Then let us suppose that $a_i = \frac{i+1}{2^i}$ for all

$i = 1, \ldots, n$.

$$\begin{aligned}
a_{n+2} &= \frac{3}{2(n+1)(n+2)} \sum_{i=0}^{n} a_i a_{n-i} \\
&= \frac{3}{2(n+1)(n+2)} \sum_{i=0}^{n} \frac{i+1}{2^i} \frac{n-i+1}{2^{n-i}} \\
&= \frac{3}{2^{n+1}(n+1)(n+2)} \sum_{i=0}^{n} (i+1)(n-i+1) \\
&= \frac{3}{2^{n+1}(n+1)(n+2)} \sum_{i=0}^{n} (in + n - i^2 + 1) \\
&= \frac{3}{2^{n+1}(n+1)(n+2)} \left[n\frac{n(n+1)}{2} + n(n+1) - \frac{n(n+1)(2n+1)}{6} + (n+1) \right] \\
&= \frac{3}{2^{n+1}(n+2)} \left[\frac{n^2}{2} + n - \frac{n(2n+1)}{6} + 1 \right] \\
&= \frac{1}{2^{n+2}(n+2)} \left[3n^2 + 6n - n(2n+1) + 6 \right] \\
&= \frac{1}{2^{n+2}(n+2)} \left[n^2 + 5n + 6 \right] \\
&= \frac{1}{2^{n+2}(n+2)} (n+2)(n+3) \\
&= \frac{n+3}{2^{n+2}}.
\end{aligned}$$

Therefore, the recurrence formula holds for $\lambda = 1$.

We will prove now the first assertion for any λ. If we write $b_n = \lambda a_n$, the recursive relation becomes :

$$b_{n+2} = \frac{3}{2(n+1)(n+2)} \sum_{i=0}^{n} b_i b_{n-i}.$$

Thus, if $a_0 = a_1 = \frac{1}{\lambda}$, that is, if $b_0 = b_1 = 1$, then $b_n = \frac{n+1}{2^n}$ (we are in the case $\lambda = 1$), and then

$$a_n = \frac{b_n}{\lambda} = \frac{n+1}{2^n \lambda}.$$

Let us prove now the second assertion, for any λ. If we write

$$b_n = \frac{a_n}{\lambda^{\frac{n}{2}}},$$

then the relation becomes :

$$b_{n+2} = \frac{3}{2(n+1)(n+2)} \sum_{i=0}^{n} b_i b_{n-i}.$$

Since $a_0 = 1$ and $a_1 = \lambda^{\frac{1}{2}}$, we have $b_0 = b_1 = 1$ and so $b_n = \frac{n+1}{2^n}$. So we have :

$$a_n = \frac{n+1}{2^n} \lambda^{\frac{n}{2}}.$$

$\diamond$

Lemma 7.15 *Let K be an algebraically closed field of characteristic zero. Let q be an element of K different from 0. Let (a_n) be the sequence defined by $a_0 = -23$, and*

$$a_n = \frac{n+1}{2^n q^n}, \quad n \geq 1.$$

Then the power series

$$H = \sum_{n \geq 0} a_n T^n$$

satisfies the following relation:

$$(H')^2 = \lambda H^3 + \gamma H^2 + \mu H$$

where $\lambda = \frac{1}{q^2}$, $\gamma = 2^3 \cdot 3^2 \lambda$ and $\mu = 2^6 \cdot 3^3 \lambda$.

Proof: Note that $a_0 = 1 - \frac{q^2\gamma}{3}$. By Lemma 7.2, it suffices to show that:

$$\begin{aligned}
a_1^2 &= \lambda a_0^3 + \gamma a_0^2 + \mu a_0 \\
a_2 &= \frac{1}{4}(3\lambda a_0^2 + 2\gamma a_0 + \mu) \\
a_{n+2} &= \frac{1}{2(n+1)(n+2)} \left(3\lambda \sum_{i=0}^{n} a_i a_{n-i} + 2\gamma a_n \right), \quad \text{n} \geq 1.
\end{aligned}$$

Define the sequence (b_n), $n \geq 0$, by taking $b_n = a_n$, for $n \geq 1$, and $b_0 = a_0 + \frac{\gamma}{3\lambda}$. We will show that (a_n) satisfies the stated recursive relation if and only if b_n satisfies the relation:

$$b_{n+2} = \frac{3\lambda}{2(n+1)(n+2)} \sum_{i=0}^{n} b_i b_{n-i}, \quad \text{n} \geq 1.$$

We have $b_2 = a_2 = \frac{1}{4}(3\lambda a_0^2 + 2\gamma a_0 + \mu)$. By the hypothesis on the coefficients, we have $3\mu\lambda = \gamma^2$. Therefore we have:

$$\begin{aligned}
\frac{3\lambda}{4}{b_0}^2 &= \frac{3\lambda}{4}(a_0 + \frac{\gamma}{3\lambda})^2 \\
&= \frac{3\lambda}{4}({a_0}^2 + 2a_0\frac{\gamma}{3\lambda} + \frac{\gamma^2}{(3\lambda)^2}) \\
&= \frac{1}{4}(3\lambda a_0^2 + 2a_0\gamma + \frac{\gamma^2}{3\lambda}) \\
&= \frac{1}{4}(3\lambda a_0^2 + 2\gamma a_0 + \mu) \\
&= b_2
\end{aligned}$$

The way we chose b_0 makes it equal to 1, by using the hypothesis on a_0. Let us prove now that

$$b_1 = \pm\lambda^{\frac{1}{2}} = \pm\frac{1}{q}.$$

We have :

$$\begin{aligned}
b_1^2 - \lambda &= a_1^2 - \lambda \\
&= \lambda a_0^3 + \gamma a_0^2 + \mu a_0 - \lambda \\
&= \lambda \left(1 - \frac{\gamma}{3\lambda}\right)^3 + \gamma \left(1 - \frac{\gamma}{3\lambda}\right)^2 + \mu \left(1 - \frac{\gamma}{3\lambda}\right) - \lambda \\
&= \lambda(1 - \frac{\gamma}{\lambda} + 3\frac{\gamma^2}{\lambda^2} - \frac{\gamma^3}{3^3\lambda^3}) + \gamma(1 - 2\frac{\gamma}{3\lambda} + \frac{\gamma^2}{3^2\lambda^2}) + \mu(1 - \frac{\gamma}{3\lambda}) - \lambda \\
&= -\gamma + 3\frac{\gamma^2}{\lambda} - \frac{\gamma^3}{3^3\lambda^2} + \gamma - \frac{2\gamma^2}{3\lambda} + \frac{\gamma^3}{3^2\lambda^2} + \mu - \frac{\mu\gamma}{3\lambda} \\
&= (3 - \frac{2}{3})\frac{\gamma^2}{\lambda} + (-1+3)\frac{\gamma^3}{3^3\lambda^2} + \mu - \frac{\mu\gamma}{3\lambda} \\
&= 8\mu + \frac{2}{3^3}\frac{\gamma^3}{\lambda^2} - \frac{\mu\gamma}{3\lambda} \\
&= 8\mu + \frac{2\gamma}{3^2\lambda}.\frac{\gamma^2}{3\lambda} - \frac{\mu\gamma}{3\lambda} \\
&= 8\mu + \frac{2\gamma}{3^2\lambda}\mu - \frac{\mu\gamma}{3\lambda} \\
&= 8\mu - \frac{\mu\gamma}{3^2\lambda} \\
&= 8 \cdot 2^6 \cdot 3^3\lambda - \frac{2^6 \cdot 3^3\lambda \cdot 2^3 \cdot 3^2\lambda}{3^2\lambda} \\
&= 0.
\end{aligned}$$

Now, choosing $b_1 = \lambda^{\frac{1}{2}}$, we can apply the second assertion of Lemma 7.14 to the sequence b_n to conclude. ◇

Applying Lemma 7.15 with $K = \mathbf{C}_p$ and, for instance, $q = p$, we get a Weierstrass power series H which has a positive radius of convergence. Note that whatever we choose q to be, the radius of convergence of H will be finite, because by changing the value of q, we get an isomorphic elliptic curve. In the complex case however, we see that the radius of convergence of H is infinite (for any q).

7.3 Factorization of formal parametrizations (for composition)

In this subsection, (X, Y) will be a Laurent solution of (1), with $Y \neq 0$. By Corollary 7.3, there exists at least one such solution.

Lemma 7.16 *The quotient $\frac{X'}{Y}$ is a formal power series, that is, $\frac{X'}{Y} \in K[[T]]$.*

Proof: Let us suppose first that $\mathcal{V}(X)$ is negative. Since we have :

$$2\mathcal{V}(Y) = \mathcal{V}(Y^2) = \mathcal{V}(X^3 + \delta X^2 + X) = 3\mathcal{V}(X),$$

the integer $\mathcal{V}(X)$ must be even, then less than or equal to -2. Hence we have :

$$\mathcal{V}\left(\frac{X'}{Y}\right) = \mathcal{V}(X') - \mathcal{V}(Y) = \mathcal{V}(X) - 1 - \frac{3\mathcal{V}(X)}{2} = \frac{-\mathcal{V}(X) - 2}{2} \geq 0$$

So, from now on, we assume that $\mathcal{V}(X) \geq 0$.

Let us suppose that $\mathcal{V}(Y)$ is positive. We have:

$$\mathcal{V}(X^3 + \delta X^2 + X) = \mathcal{V}(Y^2) = 2\mathcal{V}(Y) > 0.$$

Since the polynomials $T^3 + \delta T^2 + T$ and $3T^2 + 2\delta T + 1$ are coprime, we have

$$\mathcal{V}(3X^2 + 2\delta X + 1) = 0.$$

By differentiating Equation (1), and applying the valuation $\mathcal{V}$, we obtain:

$$2\mathcal{V}(Y) - 1 = \mathcal{V}\left((X^3 + \delta X^2 + X)'\right) = \mathcal{V}(X') + \mathcal{V}(3X^2 + 2\delta X + 1) = \mathcal{V}(X'),$$

which implies that

$$\mathcal{V}(X') - \mathcal{V}(Y) = \mathcal{V}(Y) - 1.$$

Therefore, we have:

$$\mathcal{V}\left(\frac{X'}{Y}\right) = \mathcal{V}(X') - \mathcal{V}(Y) = \mathcal{V}(Y) - 1 \geq 0.$$

In the case that $\mathcal{V}(Y) = 0$, the result is obvious. ◇

Corollary 7.17 *Let (X, Y) be a Laurent solution of Equation (1), with $\mathcal{V}(X) = \pm 2$. Then there exists a unique power series $U \in K[[T]]$ such that $\mathcal{V}(U) = 1$ and $U' = \frac{X'}{Y}$.*

Proof: If $\mathcal{V}(X) = -2$, then, by looking at Equation (1), we find $\mathcal{V}(Y) = -3$, and we obtain:

$$\mathcal{V}\left(\frac{X'}{Y}\right) = \mathcal{V}(X') - \mathcal{V}(Y) = 0.$$

If $\mathcal{V}(X) = 2$, then $\mathcal{V}(Y) = 1$, and we obtain again $\mathcal{V}\left(\frac{X'}{Y}\right) = 0$. Therefore, in both cases, we choose for U the formal integral of $\frac{X'}{Y}$ with first coefficient equal to zero. ◇

Lemma 7.18 *Let U be a power series such that $\mathcal{V}(U) = 1$ and let W be any power series in $K[[T]]$. There exists a unique power series $H \in K[[T]]$ such that*

$$W = H \circ U.$$

Proof: This is a direct consequence of Lemma 6.8. ◇

Corollary 7.19 *Let U be a power series such that $\mathcal{V}(U) = 1$ and let W be any Laurent series in $K((T))$. There exists a unique Laurent series $H \in K((T))$ such that*

$$W = H \circ U.$$

Proof: We write $W = \frac{W_0}{W_1}$ for some power series W_0 and W_1, and we apply Lemma 7.18 to W_0 and W_1. ◇

Theorem 7.20 *Let (X, Y) be a Laurent solution of Equation (1), with $\mathcal{V}(X) = -2$. Let $U \in K[[T]]$ such that $\mathcal{V}(U) = 1$ and $U' = \frac{X'}{Y}$ (see Corollary 7.17). Then we have*

$$(X, Y) = (P, P') \circ U,$$

where P is the Weierstrass Laurent series of $\mathcal{E}$ (see subsection 7.1).

Proof: By Corollary 7.19, there exists a Laurent series H in $K((T))$ such that

$$X = H \circ U.$$

By differentiating this expression, we find

$$X' = U' \cdot (H' \circ U) = \frac{X'}{Y} \cdot (H' \circ U),$$

and then

$$Y = H' \circ U.$$

Since $\mathcal{V}(U) = 1$, the formal inverse $\overset{-1}{U}$ of U exists (see Lemma 6.8), and satisfies:

$$\mathcal{V}(\overset{-1}{U}) = \mathcal{V}(U) \cdot \mathcal{V}(\overset{-1}{U}) = \mathcal{V}(U \circ \overset{-1}{U}) = 1.$$

Since (X, Y) satisfies Equation (1), the pair

$$(X \circ \overset{-1}{U}, Y \circ \overset{-1}{U}) = (H, H')$$

satisfies also Equation (1). Moreover, we have:

$$\mathcal{V}(H) = \mathcal{V}(X \circ \overset{-1}{U}) = \mathcal{V}(X) = -2 < 0,$$

Therefore, H is a Weierstrass strictly Laurent series, which, by Corollary 7.5, must be equal to the Weierstrass Laurent series P. ◇

Corollary 7.21 *With the same notations as in Theorem 7.20, if $\mathcal{V}(X) = 2$, then we have:*

$$(X, Y) = (Q, Q') \circ U,$$

where Q is the Weierstrass power series of $\mathcal{E}$ (see subsection 7.1).

Proof: We define the Laurent series $S = \frac{1}{X}$ and $T = \frac{Y}{X^2}$; they are solutions of Equation (1). We have $\mathcal{V}(S) = -2$, and $\frac{S'}{T} = -\frac{X'}{Y} = -U'$. We apply Theorem 7.20 to (S, T) and we obtain:

$$(S, T) = (P, P') \circ (-U).$$

In particular, we have:

$$X = \frac{1}{S} = \frac{1}{P \circ (-U)} = Q \circ U$$

and

$$Y = \frac{T}{S^2} = \frac{P' \circ (-U)}{(P \circ (-U))^2} = \frac{P'}{P^2} \circ (-U) = Q' \circ U.$$

◇

Corollary 7.22 *If $\mathcal{V}(X) = -2$, then, for any positive integer n we have:*

$$n(X, Y) = (P, P') \circ (nU).$$

Proof: This follows from Theorem 7.20 and Corollary 7.9. We have:

$$n(X, Y) = n[(P, P') \circ U] = [n(P, P')] \circ U = [(P, P') \circ (n\mathrm{Id})] \circ \mathrm{U} = (\mathrm{P}, \mathrm{P}') \circ (\mathrm{nU}).$$

◇

7.4 Local meromorphic parametrizations : Properties

Let (Γ, Θ) denote the Laurent solution described in subsection 7.2. Since $\mathcal{V}(\Gamma) = 2$ (see Corollary 7.11, 2), we can apply Corollary 7.21 to (Γ, Θ). We obtain the following result of convergence :

Theorem 7.23 *The Weierstrass series Q has a positive radius of convergence.*

Proof: By Corollary 7.21, we have $\Gamma = Q \circ U$, where $U \in K[[T]]$ is such that $\mathcal{V}(U) = 1$, and $U' = \frac{\Gamma'}{\Theta}$. Since $\Gamma = T\Theta$, we can write

$$U' = \frac{T\Gamma'}{\Gamma} = \frac{\Gamma'}{T}\left(\frac{\Gamma}{T^2}\right)^{-1}.$$

Since $\mathcal{V}(\Gamma') = 1$, the quotient $\frac{\Gamma'}{T}$ is a power series, and it has a positive radius of convergence by Corollary 7.13 and Lemma 6.6. Since $\mathcal{V}(\frac{\Gamma}{T^2}) = 0$, the quotient $\frac{\Gamma}{T^2}$ is also a power series, convergent by Corollary 7.13; by Lemma 6.5, its formal inverse (for multiplication) is a convergent power series. Therefore, the power series U' has a positive radius of convergence, as the product of two convergent series (see Lemma 6.5). Hence, by Lemma 6.6, the power series U has a positive radius of convergence. Since $\mathcal{V}(U) = 1$, we know from Lemma 6.8 that we can invert formally the power series U, with respect to composition; so we have

$$Q = \Gamma \circ \overset{-1}{U}.$$

We apply the inverse function theorem (see 6.10) to U and we conclude that $\overset{-1}{U}$ has a positive radius of convergence. Then $Q = \Gamma \circ \overset{-1}{U}$ has a positive radius of convergence by Lemma 6.5 (note that $\mathcal{V}(\overset{-1}{U}) = 1$). ◇

We will denote by $\mathbf{D}$ the disc of convergence of Q around 0, and by $\mathcal{Q}$ the analytic function defined by Q on $\mathbf{D}$. Then $\mathcal{Q}$, as an analytic function, is maximal (see Definition 6.13). Note that, up to this point, we do not know whether the radius of $\mathbf{D}$ is finite or not; the Weierstrass series Q might have an infinite radius of convergence (this was not the case for the particular Weierstrass series we have computed in subsection 7.2).

Define $\mathcal{P}_0 = \frac{1}{\mathcal{Q}} \in \mathcal{M}_p(\mathbf{D})$. The expansion of $\mathcal{P}_0$ around 0 is given by the Weierstrass Laurent series P (see Lemma 6.11, 4). We will denote by $\mathcal{P}$ the maximal meromorphic function whose expansion around zero is P and by $\mathbf{D}_{\mathcal{P}}$ the disc on which $\mathcal{P}$ is defined (as a meromorphic function). Hence the disc $\mathbf{D}_{\mathcal{P}}$ contains the disc $\mathbf{D}$ and then a zero of the function $\mathcal{Q}$ must be a pole of $\mathcal{P}$. We do not have a priori the inverse inclusion. The function $\mathcal{P}$ might be the quotient of two analytic functions defined on a disc containing strictly $\mathbf{D}$. So we do not know a priori if a pole of $\mathcal{P}$ is a zero of $\mathcal{Q}$. We will see that, actually, the discs $\mathbf{D}_{\mathcal{P}}$ and $\mathbf{D}$ are the same (see Corollary 7.28).

Definition 7.24 We will call $\mathcal{Q}$ *the Weierstrass analytic function (of $\mathcal{E}$)* and $\mathcal{P}$ *the Weierstrass function (of $\mathcal{E}$).*

Remark 7.25 Since (P, P') satisfies Equation (1), the pair $(\mathcal{P}_0, \mathcal{P}_0')$ satisfies also Equation (1) (see Corollary 6.12), and then the pair $(\mathcal{P}, \mathcal{P}')$ satisfies Equation (1) (see Lemma 6.14).

Lemma 7.26 *The Weierstrass function $\mathcal{P}$ has no other pole than* 0. *As a consequence, its derivative $\mathcal{P}'$ has no other pole than* 0 *and has no zero, the function $\mathcal{P}$ has no zero, and the Weierstrass analytic function $\mathcal{Q}$ has no zero other than* 0.

Proof: Suppose that $\mathcal{P}$ has a pole $\rho \neq 0$. By Lemma 7.9, we have:

$$2(P, P') = (P, P') \circ (2\mathrm{Id}).$$

By the addition formula, we obtain

$$\frac{(P^2-1)^2}{4P'^2} = P \circ (2\mathrm{Id}).$$

Since for any $z \in \mathbf{C}_p$ we have $|2z|_p \leq |z|_p$, this formal relation is true on $\mathbf{D}$ if we replace P by $\mathcal{P}_0$ (see Corollary 6.12, together with Remark 7.25), and then it is true on $\mathbf{D}_{\mathcal{P}}$ if we replace $\mathcal{P}_0$ by $\mathcal{P}$ (see Lemma 6.14). So we have:

(Duplication formula) $$\frac{(\mathcal{P}^2-1)^2}{4\mathcal{P}'^2} = \mathcal{P} \circ (2\mathrm{Id}).$$

Since ρ is a pole of $\mathcal{P}$, it is a pole of order -2 (see Remark 7.25 and compute the order at ρ of $\mathcal{P}$ and $\mathcal{P}'$ using Equation (1)), then it is also a pole of order $-2 \cdot 4 + 2 \cdot 3 = -2$ of

$$\frac{(\mathcal{P}^2-1)^2}{4\mathcal{P}'^2},$$

and then, by the duplication formula, 2ρ is a pole of $\mathcal{P}$. Therefore, by repeating the operation, we see that for any positive integer n, $2^n\rho$ is a pole of $\mathcal{P}$. If $p = 2$, then $\mathcal{P}$ has a sequence of poles whose 2-adic absolute value goes to zero, which is impossible by Lemma 6.14. If $p \neq 2$, we obtain infinitely many distinct poles of $\mathcal{P}$, all having the same absolute value, and we get a contradiction, again by Lemma 6.14. So $\mathcal{P}$ has no pole other than 0.

The fact that $\mathcal{Q}$ has no other zero than 0 is then obvious, by definition.

Now we will prove that $\mathcal{P}'$ has no zero. The roots of the polynomial $T^3 + \delta T^2 + T$ are 0, and

$$\frac{-\delta \pm \sqrt{\delta^2 - 4}}{2}.$$

Therefore the polynomials $T^3 + \delta T^2 + T$ and $T^2 - 1$ have no common roots, since we have chosen $\delta^2 \neq 4$. Hence the functions $\mathcal{P}^3 + \delta\mathcal{P}^2 + \mathcal{P}$ and $\mathcal{P}^2 - 1$ have no common zeros; by Remark 7.25, it means that the functions $\mathcal{P}'^2$ and $\mathcal{P}^2 - 1$ have no common zeros. Then, by the duplication formula for $\mathcal{P}$, we have the following: if ρ is a zero of $\mathcal{P}'$ then 2ρ is a pole of $\mathcal{P}$. Therefore, the only possible zero of $\mathcal{P}'$ would be 0, but 0 is a pole of $\mathcal{P}$, so of $\mathcal{P}'$.

We see from Equation (1) that a zero of $\mathcal{P}$ must be a zero of $\mathcal{P}'$. As a result the Weierstrass function $\mathcal{P}$ has no zero. ◇

Corollary 7.27 *The Weierstrass function $\mathcal{P}$ is not a global meromorphic function. The Weierstrass function $\mathcal{Q}$ is not a global analytic function.*

Proof: Since $\mathcal{P}$ has only one pole and no zero, we know from Lemma 6.19 that either it is not global or it is a rational function. But it is known that curves of genus 1 cannot be parametrized by rational functions (see for example [26]).

Similarly, since $\mathcal{Q}$ has only one zero and is not a polynomial, it cannot be a global analytic function. ◇

Corollary 7.28 *The discs $\mathbf{D}_{\mathcal{P}}$ and $\mathbf{D}$ are the same.*

Proof: Since $\mathcal{P}$ has only one pole at 0 and no zero, its inverse $\frac{1}{\mathcal{P}}$ is an analytic function on $\mathbf{D}_{\mathcal{P}}$, which is equal to $\mathcal{Q}$ on $\mathbf{D}$. Since $\mathcal{Q}$ is maximal, we have $\mathbf{D}_{\mathcal{P}} \subseteq \mathbf{D}$. As we saw previously, the other inclusion follows from the maximality of $\mathcal{P}$. ◇

We will denote by $r = \mathrm{RC}(\mathbf{Q})$ the radius of the disc $\mathbf{D}$. The following lemma is a direct consequence of the p-adic Weierstrass preparation theorem (see [25, Thm. 6.3.10, p.194]). It will permit us to bound the value of r.

Lemma 7.29 *Let $H = \sum_{n \geq 0} h_n T^n$ be a power series which converges on $\bar{D}(0,c)$ and let h be the function defined by H on the disc $\bar{D}(0,c)$. Let N be the number of zeros (counted with multiplicity) of h in $\bar{D}(0,c)$. Then N satisfies the following property :*

$$(\star) \qquad |h_N|_p c^N = \max_n |h_n|_p c^n \quad \text{and} \quad \forall n > N, |h_n|_p c^n < |h_N|_p c^N.$$

Proof: Actually, the theorem says that the integer N which satisfies the property $(\star)$ is the number of zeros of h in $\bar{D}(0,c)$ (see also [25, problem 287]). ◇

Corollary 7.30 *Write the Weierstrass power series Q as $Q = \sum_{n \geq 2} q_n T^n$, with $q_n \in \mathbf{Q}[\delta]$. Then we have, for all integers $n > 2$ such that $q_n \neq 0$:*

$$r = \mathrm{RC(Q)} \leq \frac{\sqrt[n-2]{|q_2|_p}}{\sqrt[n-2]{|q_n|_p}}.$$

Proof: We apply Lemma 7.29 to any disc $\bar{D}(0, r_0)$, with $r_0 < r$. The integer N is equal to 2 in our case, since $\mathcal{Q}$ has only one zero of multiplicity 2. Then we have for all integers $n > 2$:

$$|q_n|_p r_0^n < |q_2|_p r_0^2.$$

◇

From Lemma 7.2, it is easy to compute the first coefficients of the Weierstrass power series $\mathcal{Q}$. We obtain then the following corollary (note that we may obtain better bounds by looking at further coefficients of $\mathcal{Q}$).

Corollary 7.31 *We have :*

1. *if $\delta = 0$ and $p \neq 2$, then $r < 1$;*
2. *if $\delta = 0$ and $p = 2$, then $r < \frac{1}{2}$;*
3. *if $\delta \neq 0$ and $p \neq 2$, then :*
$$r < \sqrt{\frac{|3|_p}{|\delta|_p}} \, ;$$
4. *if $\delta \neq 0$ and $p = 2$, then :*
$$r < \frac{1}{2\sqrt{|\delta|_2}}.$$

7.5 Proof of Theorem 7.1 : no global meromorphic parametrization exists

We have seen in subsection 6.6 that any elliptic curve is isomorphic to one whose affine equation is of the form :

$$(1) \qquad\qquad y^2 = x^3 + \delta x^2 + x.$$

We suppose that there exists a non-constant global meromorphic solution (x, y) of Equation (1). This will lead to a contradiction.

Lemma 7.32 *Let $x \in \mathcal{M}_p - \mathbf{C}_p$. The set of constants a in $\mathbf{C}_p$ such that the function $x - a$ has a simple zero is non-discrete.*

Proof: Write $\mathrm{Im}\,(x)$ the image of $\mathbf{C}_p$ through x. Suppose that the set

$$\{a \in \mathbf{C}_p \mid \text{there exists } \rho \in \mathbf{C}_p, \text{ such that } x(\rho) = a \text{ and } x'(\rho) \neq 0\} \subset \mathrm{Im}\,(x).$$

is discrete. Then its complement in $\mathrm{Im}\,(x)$,

$$A = \{a \in \mathbf{C}_p \mid \text{for all}\, \rho \in \mathbf{C}_p,\ x(\rho) = a \text{ implies } x'(\rho) = 0\} \cap \mathrm{Im}\,(x)$$

is non-discrete, since the image of a non-constant meromorphic function is non-discrete (see Corollary 6.16). Since $A \subset \mathrm{Im}\,(x)$, to any element a of A corresponds at least one ρ such that $x(\rho) = a$, and then $x'(\rho) = 0$. Therefore, the set

$$\{\rho \in \mathbf{C}_p \mid x'(\rho) = 0\}$$

is non-discrete. This implies that $x' = 0$ (see Lemma 6.14), which contradicts the fact that x is a non-constant meromorphic function (see Lemma 6.15). ◇

Corollary 7.33 *Let $(x, y) \in \mathcal{E}(\mathcal{M}_p) - \infty$, with $x, y \notin \mathbf{C}_p$. We can choose $(a, b) \in \mathcal{E}(\mathbf{C}_p)$ such that, if $(r, s) = (x, y) \oplus (a, b)$, then r has a pole of multiplicity 2.*

Proof: Choose a constant a which is not a root of the polynomial $T^3 + \delta T^2 + T$, and let $\rho \in \mathbf{C}_p$ be such that $x(\rho) = a$ and $x'(\rho) = 0$ (by Lemma 7.32, such a constant exists). Note that, since (x, y) satisfies Equation (1), ρ cannot be a pole of y. There are two distinct constants b such that (a, b) is on the elliptic curve, because

$$b^2 = a^3 + \delta a^2 + a \neq 0.$$

At least one of these two constants b is not equal to $y(\rho)$; we choose that one. Let $(r, s) = (x, y) \oplus (a, b)$. By the addition formula, we have:

$$r = \left(\frac{y - b}{x - a}\right)^2 - \delta - x - a.$$

It is obvious that ρ is a pole of r of order -2. ◇

According to Corollary 7.33, there is an $(a, b) \in \mathcal{E}(\mathbf{C}_p) - \infty$ such that $(r, s) = (x, y) \oplus (a, b)$ has the property that the order of r at some point $\rho \in \mathbf{C}_p$ is equal to -2. Then, obviously, $(r(z - \rho), s(z - \rho)) \in \mathcal{E}(\mathcal{M}_p) - \mathcal{E}(\mathbf{C}_p)$ and $\mathrm{ord}_0(r(z - \rho)) = -2$. So, from now on, we assume, without loss of generality, that the given solution (x, y) satisfies $\mathrm{ord}_0(x) = -2$.

If ρ is any element of $\mathbf{C}_p$, let us denote by X_ρ and Y_ρ respectively the Laurent series expansion around ρ of the meromorphic function x and y. Since (x, y) satisfies Equation (1), the pair (X_ρ, Y_ρ) satisfies also Equation (1), for any ρ. Then the quotient $\frac{X'_\rho}{Y_\rho}$ is a formal power series, that is, it belongs to the ring $\mathbf{C}_p[[T]]$ (see Lemma 7.16). Therefore, the quotient $\frac{x'}{y}$ is a global meromorphic function without pole, (because, by Lemma 6.11, 4, the formal quotient $\frac{X'_\rho}{Y_\rho}$ is the expansion of $\frac{x'}{y}$ around ρ), that is, a global analytic function (see Lemma 6.19). Thus, for any ρ, the quotient $\frac{X'_\rho}{Y_\rho}$ has an infinite radius of convergence (by definition of analytic functions and by Lemma 6.1).

When $\rho = 0$, we will write respectively X and Y instead of X_ρ and Y_ρ.

By Corollary 7.17, there exists a unique power series U such that $\mathcal{V}(U) = 1$ and $U' = \frac{X'}{Y}$. By Lemma 6.6, the power series U has an infinite radius of convergence. Let us denote by u the entire analytic function defined by U.

By Corollary 7.22, we have for any integer n

$$n(X, Y) = (P, P') \circ (nU),$$

where P and P' are the Weierstrass Laurent series and its derivative (see Definition 7.7 in subsection 7.1). It is clear, considering the addition formula on the elliptic curve $\mathcal{E}$, that if $(S, T) = n(X, Y)$, then S and T are rational functions in the variables X and Y. Note also that, for any $z \in \overset{-1}{(nu)} (\mathbf{D})$, we have (see subsection 7.4 for the definition and some properties of $\mathbf{D}$):

$$(n(x, y))\,|_z = n\left((x, y)|_z\right).$$

Therefore, by Corollary 6.12, we have, for any integer n, the equality of functions

$$n(x, y) = (\mathcal{P}, \mathcal{P}') \circ (nu)$$

on $\overset{-1}{(nu)} (\mathbf{D})$. Note that the set $\overset{-1}{(nu)} (\mathbf{D})$ gets bigger as the integer n grows (because we have $|n|_p \leq 1$).

Remark 7.34 The latter equality, for $n = 1$, implies that a zero of u is a pole of x and y.

Suppose now that for some $\rho \in \mathbf{C}_p$,

$$(x, y)|_{z=\rho}$$

is a point of order n on the elliptic curve. Let r denote the radius of $\mathbf{D}$. There exists a non-zero integer m, multiple of n, such that $|mu(\rho)|_p$ is strictly less than r. Then we have:

$$\infty = m(x, y)|_{z=\rho} = (\mathcal{P}, \mathcal{P}') \circ (mu)|_{z=\rho}.$$

Since $\mathcal{P}$ and $\mathcal{P}'$ have only one pole at 0, ρ must be a zero of mu, hence of u. Therefore, by Remark 7.34, ρ is a pole of x and y, that is, the point $(x, y)|_{z=\rho}$ is a point of order 1. So the integer n must be equal to 1.

In other words, the function (x, y) cannot reach any point of order more than 1 on $\mathcal{E}$. In particular, (x, y) cannot reach any of the three points of order 2 of $\mathcal{E}$. If ξ and ξ^{-1} are the roots of the polynomial $X^2 + \delta X + 1$, the points of order 2 of $\mathcal{E}$ are:

$$(0, 0), \qquad (\xi, 0) \qquad \text{and} \qquad (\xi^{-1}, 0).$$

But when the function x takes one of the three values 0, ξ, or ξ^{-1}, the function y takes necessarily the value 0 (because (x, y) satisfies Equation (1)). Thus the function x cannot reach any of the three values 0, ξ, or ξ^{-1}. This implies, by Lemma 6.19, that x is constant. This contradicts our hypothesis and proves the theorem.

8 Existential definability of the integers in $\mathcal{M}_p$

Let F denote the polynomial

$$F(T) = T^3 + \delta T^2 + T$$

where δ is any fixed constant in $\mathbf{C}_p$, such that $\delta^2 \neq 4$. We will prove that the only solutions (x, y), with x and y in $\mathcal{M}_p$, of:

$$\text{(MD)} \qquad F(z)y^2 = F(x),$$

are rational functions (see Theorem 8.24, below).

Let $\mathcal{L}_R$ be the language of rings. Let $\mathcal{L}_R^*$ denote the augmentation of $\mathcal{L}_R$ by a constant symbol for the variable z and a symbol for the unary relation "$\mathrm{ord}_0(x) > 0$". The techniques developed by J. Denef in [11, part 3] will allow us to conclude that:

Theorem 8.1 *The set of rational integers is existentially definable in the field $\mathcal{M}_p$ of global meromorphic functions, in the language $\mathcal{L}_R^*$.*

By the fact that the existential theory of the set of rational integers is undecidable (see [34] or [35]), we have the following corollary.

Theorem 8.2 *The positive existential theory of the field $\mathcal{M}_p$ in the language $\mathcal{L}_R^*$ is undecidable.*

We will start by proving a few general lemmas concerning the speed of convergence of p-adic sequences. Then we will study some properties of global analytic and meromorphic functions on $\mathbf{C}_p^* = \mathbf{C}_p - \{0\}$.

8.1 Relation between the speeds of convergence of the general term and of the partial sums of a power series.

One major difference between complex analysis and p-adic analysis is that, in the p-adic case, a power series 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 formal power series.

Proposition 8.3 *Let $(h_n)_{n\geq 0}$ be a sequence of elements of $\mathbf{C}_p$ such that $\sqrt[n]{|h_n|_p}$ 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 $\sqrt[n]{|S_n - S|_p}$ converges to 0 as n goes to infinity.*

Proof: Clearly S is the limit of S_n (it exists by Lemma 6.2). We will show that

$$\lim_{n\to\infty} \sqrt[n]{|S_n - S|_p} = 0.$$

If there exists an integer N such that $h_n = 0$ for all $n \geq N$, then the quantity $|S_n - S|_p$ is 0 for $n \geq N$, and the lemma is obvious in this case. Now suppose that for infinitely many n, h_n is non-zero. We build the sequence c_n of real numbers such that:

1. If $h_n = 0$, then $c_n = c_{n+1}$.

2. If $h_n \neq 0$, then $h_n = p^{c_n} k_n$ (see subsection 6.2), where k_n has p-adic absolute value 1.

Then, if $h_n \neq 0$ (which happens for infinitely many n), we have:

$$\sqrt[n]{|h_n|_p} = \sqrt[n]{p^{-c_n}} = p^{-\frac{c_n}{n}}.$$

This fact and the way we built c_n show that the sequence $\frac{c_n}{n}$ tends to infinity. For any integer n, we have:

$$\begin{aligned} \sqrt[n]{|S_n - S|_p} &= \sqrt[n]{\left|\sum_{i \geq n+1} h_i\right|_p} \\ &\leq \sqrt[n]{\max_{i \geq n+1} |h_i|_p} \\ &= \sqrt[n]{\max_{j \geq 1} |h_{n+j}|_p} \\ &= \sqrt[n]{|p^{c_{n+j_0}}|_p} \end{aligned}$$

for some integer $j_0 \geq 1$ (see Lemma 6.3). Note that the integer j_0 depends a priori on n, but only the fact that it is positive matters:

$$\sqrt[n]{|S_n - S|_p} \leq p^{-\frac{c_{n+j_0}}{n}} = p^{-\frac{c_{n+j_0}}{n+j_0} \cdot \frac{n+j_0}{n}} \xrightarrow[n \to \infty]{} 0$$

◇

Corollary 8.4 *Let $\sum h_n T^n$ be a power series in $\mathbf{C}_p[[T]]$ 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, with the same proof (this is what we will need later on):

Lemma 8.5 *For any integers n and k, let $c_{n,k}$ be an element of the valuation ring of $\mathbf{C}_p$ (that is $|c_{n,k}|_p \leq 1$). Assume that $(h_n)_{n \geq 0}$ is a sequence of elements of $\mathbf{C}_p$ such that $\sqrt[n]{|h_n|_p}$ 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 $\sqrt[n]{|R_n|_p}$ converges to 0.

Proof: Note that if the $c_{n,k}$ are all 1, then we obtain Proposition 8.3, setting $R_n = S - S_{n-1}$. The proof of the generic case is similar to that of Proposition 8.3. ◇

8.2 Meromorphic functions on $\mathbf{C}_p - \{0\}$, symmetric under $z \mapsto z^{-1}$

Let $\mathbf{C}_p^*$ denote the set $\mathbf{C}_p - \{0\}$.

Definition 8.6 We will say that a function h is *a global analytic function on $\mathbf{C}_p^*$ (over $\mathbf{C}_p$)* if, for all $z \in \mathbf{C}_p^*$, we have:

$$h(z) = \sum_{n \in \mathbf{Z}} h_n z^n$$

for some formal Laurent series $\sum_{n\in\mathbf{Z}} h_n T^n \in \mathbf{C}_p[[T,T^{-1}]]$, converging everywhere in $\mathbf{C}_p^*$. We will say that a function is *global meromorphic on* $\mathbf{C}_p^*$ if it can be written as the quotient of two global analytic functions on $\mathbf{C}_p^*$.

The integral domain of global analytic functions on $\mathbf{C}_p^*$ will be denoted by $\mathcal{A}_p^*$ and the field of fractions of $\mathcal{A}_p^*$ will be denoted by $\mathcal{M}_p^*$. See [24], [30], [36] or [42, pp. 303-304 and 318-321] for more information on these objects.

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

Lemma 8.7 *Let h and f be two global meromorphic functions on $\mathbf{C}_p$. If for any non-zero z in $\mathbf{C}_p$, we have $h(z) = f(z^{-1})$, then the functions h and f are rational functions. If the functions h and f are global analytic functions on $\mathbf{C}_p$, 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 h has infinitely many zeros (resp. poles). Then it has a sequence ϱ_n of zeros (resp. poles) whose absolute value tends to infinity (see Lemma 6.19). 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 for p-adic meromorphic functions (see Lemma 6.14). Consequently, h, therefore f as well, has finitely many zeros and finitely many poles. By Lemma 6.19, they must be rational functions. This finishes the proof of the first assertion.

Now, if the functions h and f are global analytic on $\mathbf{C}_p$, from the first assertion, they are rational functions, therefore polynomials. It is clear then that h and f cannot satisfy $h(z) = f(z^{-1})$ if they are not constant. $\diamond$

Corollary 8.8 *Let*

$$h = \sum_{n\in\mathbf{Z}} a_n z^n$$

be a non-zero global analytic function on $\mathbf{C}_p^*$, invariant under $z \mapsto z^{-1}$. Then, for all $n \in \mathbf{Z}$, we have $a_n = a_{-n}$.

Proof: We have

$$\sum_{n\in\mathbf{Z}} a_n z^n = h(z) = h(z^{-1}) = \sum_{n\in\mathbf{Z}} a_n z^{-n}.$$

It is known that the expansion of such series is unique. See [36, chap. II, p. 14] which refers to [30]. $\diamond$

Definition 8.9 Let $h = \sum_{n\in\mathbf{Z}} a_n z^n$ be a function in $\mathcal{A}_p^*$. Three cases can occur:

- $a_n = 0$ for all $n < 0$; we then say that the origin is a *removable singularity.*
- Finitely many a_n, for $n < 0$, are non-zero; we say that the origin is a *pole.*
- Infinitely many a_n are non-zero, for $n < 0$; we say that the origin is an *essential singularity.*

We have an analogue of Lemma 6.17 for functions in $\mathcal{A}_p^*$.

Lemma 8.10 *Let $h \neq 0$ be a function in $\mathcal{A}_p^*$. If h has no zero in $\mathbf{C}_p^*$, then f is a single monomial. If h has finitely many zeros in $\mathbf{C}_p^*$, then h is a polynomial in z and z^{-1}. The function h can be written as*

$$h(z) = Cz^m \prod_{|\rho|_p \geq 1} \left(1 - \frac{z}{\rho}\right)^{\nu_\rho} \prod_{|\rho|_p < 1} \left(1 - \frac{\rho}{z}\right)^{\nu_\rho},$$

the products being taken over all non-zero zeros ρ of h, the integer ν_ρ being the multiplicity of h at ρ.

Proof: See [42, chap. 6, p. 320]. $\diamond$

Remark 8.11 Like for functions in $\mathcal{A}_p$, functions in $\mathcal{A}_p^*$ can have only finitely many zeros with the same absolute value, and have no accumulation of zeros. Also we can write a function in $\mathcal{M}_p^*$ as the quotient of two functions in $\mathcal{A}_p^*$ with no common zeros. This last assertion comes from the following remark: let $h \in \mathcal{M}_p^*$ with zeros a_n of multiplicities r_n and with poles b_n of multiplicities s_n, $n \in \mathbf{Z}$. One can build functions $f, g \in \mathcal{A}_p^*$ such that the zeros of f are precisely the a_n, with multiplicities r_n, and the zeros of g are precisely the b_n with multiplicities s_n. Write $h_1 = \frac{f}{g}$. Then the function $\frac{h}{h_1} \in \mathcal{M}_p^*$ has no zero and no pole, hence it is a single monomial, say Cz^m, by Lemma 8.10. Therefore $h = Cz^m \frac{f}{g}$ and by definition, the functions g and h have no common zeros.

Lemma 8.12 *Let h be a global analytic function on $\mathbf{C}_p^*$, invariant under $z \mapsto z^{-1}$. Then there exists a unique function g, global analytic on $\mathbf{C}_p$, such that for all z in $\mathbf{C}_p^*$, g satisfies:*

$$h(z) = g(z + z^{-1}).$$

Proof: Let us write $w = z + z^{-1}$. By lemma 8.8, 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 $\sum_{n \geq 0} b_n T^n$ is a global analytic function on $\mathbf{C}_p$. 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 coefficient 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:

$$(\mathrm{S_N}) \qquad a_n = \sum_{k=0}^{[\frac{N-n}{2}]} \binom{n+2k}{k} b_{n+2k,N}, \quad \text{for}\, n = 0, \ldots, N,$$

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 $a_N = b_{N,N}$, $b_{N-1,N}$ from $a_{N-1} = \binom{N-1}{0} b_{N-1,N}$, and $b_{n,N}$ 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:

$$\begin{aligned} 0 = a_n - a_n &= \sum_{k=0}^{[\frac{N+2-n}{2}]} \binom{n+2k}{k} b_{n+2k,N+2} - \sum_{k=0}^{[\frac{N-n}{2}]} \binom{n+2k}{k} b_{n+2k,N} \\ &= \sum_{k=0}^{[\frac{N-n}{2}]} \left(\binom{n+2k}{k} (b_{n+2k,N+2} - b_{n+2k,N}) \right) + \binom{N+2}{[\frac{N+2-n}{2}]} b_{N+2,N+2}. \end{aligned}$$

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 $0 \le n \le N$:

$$b_{n,N+2} - b_{n,N} = c \cdot a_{N+2}$$

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 $\mathbf{C}_p^*$, by Lemma 6.2, the sequence $|a_k|_p$ converges to 0 as k goes to infinity. Since the coefficients $c_{n,k}$ are integers, the sequence $|c_{n,k}a_k|_p$ 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. Obviously

$$b_n = \sum_{k \geq n} c_{n,k} a_k.$$

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

$$\sum_{n \geq 0} b_n T^n \in \mathbf{C}_p[[T]].$$

By Lemma 8.5, the power series $g(T)$ has an infinite radius of convergence (apply Lemma 8.5 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 $\mathbf{C}_p$. Let us write:

$$g_N(w) = \sum_{n=0}^{N} b_n w^n.$$

On one hand, for any integer N and any $z \in \mathbf{C}_p^*$, 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:

$$\begin{aligned}
|g_N(w) - G_N(w)|_p &= \left| \sum_{n=0}^{N} b_n w^n - \sum_{n=0}^{N} b_{n,N} w^n \right|_p \\
&= \left| \sum_{n=0}^{N} (b_n - b_{n,N}) w^n \right|_p \\
&\leq \max_{n=0}^{N} \left\{ |b_n - b_{n,N}|_p |w|_p^n \right\} \\
&= \max_{n=0}^{N} \left\{ \left| \sum_{k \geq N+1} c_{n,k} a_k \right|_p . |w|_p^n \right\}.
\end{aligned}$$

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

$$|g_N(w) - G_N(w)|_p \leq \left| \sum_{k \geq N+1} c_{u(N),k} \cdot a_k \right|_p |w|_p^{u(N)} = |R_{N+1}|_p \cdot |w|_p^{u(N)},$$

where

$$R_{N+1} = \sum_{k \geq N+1} c_{u(N),k} \cdot a_k.$$

Apply Lemma 8.5 with n replaced by $N + 1$ and h_k replaced by a_k, to obtain:

- If $|w|_p < 1$ then we have: $|R_{N+1}|_p \cdot |w|_p^{u(N)} \xrightarrow[N \to \infty]{} 0.$

- If $|w|_p \geq 1$ then $|w|_p^{u(N)} \leq |w|_p^N$, so

$$|R_{N+1}|_p \cdot |w|_p^{u(N)} \leq |R_{N+1}|_p \cdot |w|_p^N.$$

By Lemma 8.5, we have $\sqrt[N]{|R_{N+1}|_p} \xrightarrow[N\to\infty]{} 0$, thus

$$\sqrt[N]{|R_{N+1}|_p \cdot |w|_p^N} \xrightarrow[N\to\infty]{} 0,$$

which implies that

$$|R_{N+1}|_p \cdot |w|_p^N \xrightarrow[N\to\infty]{} 0.$$

The unicity of g is obvious. ◇

Lemma 8.13 *Let h be a global meromorphic function on $\mathbf{C}_p^*$ invariant under the map $z \mapsto z^{-1}$. Then $h = \frac{h_1}{h_2}$ for two global analytic functions on $\mathbf{C}_p^*$, h_1 and h_2, which are invariant under $z \mapsto z^{-1}$.*

Proof: We use Lemma 8.10 and Remark 8.11. Let us write h as the quotient $\frac{h_1}{h_2}$ of two functions in $\mathcal{A}_p^*$ with no common zeros. We can suppose without loss of generality that z does not divide h_2 (see Lemma 8.10, if $m \neq 0$ in the product expansion of h_2, we multiply both h_1 and h_2 by z^{-m}). If ϱ is any element of $\mathbf{C}_p^*$ and n a positive integer, ϱ is a zero of order n of h_1 if and only if ϱ is a zero of order n of h, which happens if and only if $\frac{1}{\varrho}$ is a zero of order n of h, and this happens if and only if $\frac{1}{\varrho}$ is a zero of order n of h_1.

Let us write

$$\pi(z) = \prod_{\substack{|\rho|_p=1\\ h_1(\rho)=0}} \left(1-\frac{z}{\rho}\right)^{\nu_\rho}, \quad \pi^+(z) = \prod_{\substack{|\rho|_p>1\\ h_1(\rho)=0}} \left(1-\frac{z}{\rho}\right)^{\nu_\rho} \quad \text{and} \quad \pi^-(z) = \prod_{\substack{|\rho|_p<1\\ h_1(\rho)=0}} \left(1-\frac{\rho}{z}\right)^{\nu_\rho}$$

By Lemma 8.10, we have, for some constant C and some integer m:

$$(\bigstar) \qquad h_1(z) = Cz^m\pi(z)\pi^+(z)\pi^-(z)$$

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

$$\pi(z) = \prod_{\substack{|\rho|_p=1\\ h_1(\rho)=0}} \left(1-\frac{z}{\rho}\right)^{\nu_\rho} = \prod_{\substack{|\mu|_p=1\\ h_1(\mu)=0}} (1-z\mu)^{\nu_\mu} = \pi(z^{-1}),$$

$$\pi^+(z) = \prod_{\substack{|\rho|_p>1\\ h_1(\rho)=0}} \left(1-\frac{z}{\rho}\right)^{\nu_\rho} = \prod_{\substack{|\mu|_p<1\\ h_1(\mu)=0}} (1-z\mu)^{\nu_\mu} = \pi^-(z^{-1})$$

and

$$\pi^-(z) = \prod_{\substack{|\rho|_p<1\\ h_1(\rho)=0}} \left(1-\frac{\rho}{z}\right)^{\nu_\rho} = \prod_{\substack{|\mu|_p>1\\ h_1(\mu)=0}} (1-\frac{1}{z\mu})^{\nu_\mu} = \pi^+(z^{-1}).$$

Therefore,

$$\frac{h_1(z)}{Cz^m} = \pi(z)\pi^+(z)\pi^-(z) = \pi(z^{-1})\pi^-(z^{-1})\pi^+(z^{-1}) = \frac{h_1(z^{-1})}{Cz^{-m}},$$

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 8.14 *Let h be a global meromorphic function on $\mathbf{C}_p^*$ invariant under $z \mapsto z^{-1}$. Then there exists a function g in $\mathcal{M}_p$ such that, for all z in $\mathbf{C}_p^*$, g satisfies $h(z) = g(z + z^{-1})$.*

Proof: By Lemma 8.13, h can be written as $\frac{h_1}{h_2}$, for some functions h_1 and h_2 in $\mathcal{A}_p^*$, invariant under $z \mapsto z^{-1}$. By lemma 8.12, there exist functions g_1 and g_2 in $\mathcal{A}_p$ such that, for all $z \in \mathbf{C}_p^*$, $h_1(z) = g_1(z + z^{-1})$ and $h_2(z) = g_2(z + z^{-1})$. Writing $g = \frac{g_1}{g_2} \in \mathcal{M}_p$, we have $h(z) = g(z + z^{-1})$. ◇

8.3 Extensions of Theorem 7.1

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

Theorem 8.15 *Let x and y be two global meromorphic functions on $\mathbf{C}_p^*$, 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 8.14, there exist functions g_1 and g_2 in $\mathcal{M}_p$ such that, for all $z \in \mathbf{C}_p^*$, $x(z) = g_1(z + z^{-1})$ and $y(z) = g_2(z + z^{-1})$. It is obvious that (g_1, g_2) satisfies the same equation as (x, y). Thus, g_1 and g_2 must be constant, since there is no parametrization over $\mathcal{M}_p$ of elliptic curves (see Theorem 7.1). Therefore, x and y must be constant. ◇

Corollary 8.16 *Let x and y be two global meromorphic functions on $\mathbf{C}_p^*$, invariant under $z \mapsto z^{-1}$, which satisfy the equation*

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

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

Proof: Write $w = z + z^{-1}$. We know by Corollary 8.14 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 Theorem 7.1 that both functions $t \cdot h \circ (t^2 - \delta)$ and $g \circ (t^2 - \delta)$ are constant. Since $h \circ (t^2 - \delta) = \frac{\text{a constant}}{t}$ is, as a function of t, both even and odd, the constant must be zero. Since $t^2 - \delta$ is surjective ($\mathbf{C}_p$ 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 $\mathcal{E}$: $(0, 0)$, $(\xi, 0)$ and $(\xi^{-1}, 0)$, where ξ is one of the non-zero roots of the polynomial F. ◇

8.4 Global meromorphic solutions of Equation (MD)

The letter F denotes the polynomial $T^3 + \delta T^2 + T$.

Remark 8.17 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 $\mathbf{C}_p(z)$ 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 $\mathcal{M}_p$, 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 $\mathcal{M}_p$. Observe that the composition of elements of $\mathcal{M}_p$ is not, in general, in $\mathcal{M}_p$. But considering a function h in $\mathcal{M}_p$ as a global meromorphic function on $\mathbf{C}_p^*$, we can compose it with the function of $\mathcal{M}_p^*$ which sends z to z^{-1}; the function $h(z^{-1})$ still lies in $\mathcal{M}_p^*$.

The map $\iota\colon z \mapsto z^{-1}$ is, obviously, an automorphism over $\mathbf{C}_p$ of the field $\mathbf{C}_p(z)$ of rational functions. This automorphism ι extends to an automorphism of the field extension $\mathbf{C}_p(z, s)$ of $\mathbf{C}_p(z)$ 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 $\mathbf{C}_p(z, s)$ which sends s to $-\frac{s}{z^2}$. Observe that, under composition, $\tilde{\iota}$ is nilpotent of order 2, that is, $\tilde{\iota} \circ \tilde{\iota}$ is the identity function.

If $(z, s) \in \mathcal{E}(\mathbf{C}_p^*)$, then the pair $(\tilde{\iota}(z), \tilde{\iota}(s))$ lies in $\mathcal{E}(\mathbf{C}_p^*)$. Therefore, to $\tilde{\iota}$ corresponds naturally a map $\tau_0\colon \mathcal{E}(\mathbf{C}_p^*) \to \mathcal{E}(\mathbf{C}_p^*)$, which sends the point (z, s) to

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

Obviously, the map τ_0 is of order 2, that is $\tau_0 \circ \tau_0$ is the identity of $\mathcal{E}(\mathbf{C}_p^*)$. Let $\tau\colon \mathcal{E}(\mathcal{M}_p) \to \mathcal{E}(\mathcal{M}_p^*)$ denote the map which sends the point (x, sy) to :

$$(x \circ z^{-1}, -\frac{s}{z^2} \cdot y \circ z^{-1}) = (x, sy) \circ \tau_0.$$

Observe that, since $\tau(x, sy)$ is a solution of Equation (1) over $\mathcal{M}_p^*$, the image of the map τ is included in $\mathcal{E}(\mathcal{M}_p^*)$. Since the map τ_0 is of order 2, the map τ, also, is of order 2.

Remark 8.18 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 τ by :

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

Lemma 8.19 *For any solution (x, y) of Equation (MD), with x and y in $\mathcal{M}_p^*$, 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 $(x, sy) \neq \tau(x, sy)$ *and* $(x, sy) \neq \ominus\tau(x, sy)$*, 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 $\tilde{y} = y \circ z^{-1}$.

1. Observe that, by the addition law on $\mathcal{E}$,

$$2(x, sy) = \left(\left(\frac{3x^2 + 2\delta x + 1}{2sy}\right)^2 - \delta - 2x, -\frac{(3x^2 + 2\delta x + 1)(x^2 - 1)^2 - 4s^2y^2(x^3 - x)}{8y^3s^3}\right)$$

So we have:

$$\begin{aligned}
&\tau(2(x, sy)) \\
&= \tau\left(\left(\frac{3x^2 + 2\delta x + 1}{2sy}\right)^2 - \delta - 2x, -\frac{(3x^2 + 2\delta x + 1)(x^2 - 1)^2 - 4s^2y^2(x^3 - x)}{8y^3s^3}\right) \\
&= \left(\left(\frac{3\tilde{x}^2 + 2\delta\tilde{x} + 1}{-2\frac{s}{z^2}\tilde{y}}\right)^2 - \delta - 2\tilde{x}, -\frac{(3\tilde{x}^2 + 2\delta\tilde{x} + 1)(\tilde{x}^2 - 1)^2 - 4\frac{s^2}{z^4}\tilde{y}^2(\tilde{x}^3 - \tilde{x})}{-8\tilde{y}^3\frac{s^3}{z^6}}\right) \\
&= 2(\tilde{x}, \frac{-s}{z^2}\tilde{y}) \\
&= 2\tau(x, sy).
\end{aligned}$$

2. Write $(a, sb) = 2(x, sy)$, $(u, v) = (a, sb) \oplus (z, s)$, $\tilde{a} = a \circ z^{-1}$ and $\tilde{b} = b \circ z^{-1}$. Note that a cannot be equal to z, because (z, s) cannot be written as the double of a solution (see Definition 8.21 and the following remark). We have:

$$\begin{aligned}
&\tau((a, sb) \oplus (z, s)) \\
&= \tau\left(\left(\frac{s - sb}{z - a}\right)^2 - \delta - z - a, -\left(\frac{s - sb}{z - a}\right)u(z, s) - \frac{sbz - as}{z - a}\right) \\
&= \left(\left(\frac{-\frac{s}{z^2} + \frac{s}{z^2}\tilde{b}}{z^{-1} - \tilde{a}}\right)^2 - \delta - z^{-1} - \tilde{a}, -\left(\frac{-\frac{s}{z^2} + \frac{s}{z^2}\tilde{b}}{z^{-1} - \tilde{a}}\right)u(z^{-1}, -\frac{s}{z^2}) - \frac{-\frac{s}{z^2}\tilde{b}z^{-1} + \tilde{a}\frac{s}{z^2}}{z^{-1} - \tilde{a}}\right) \\
&= (\tilde{a}, -\frac{s}{z^2}\tilde{b}) \oplus (z^{-1}, -\frac{s}{z^2}) \\
&= \tau(a, sb) \oplus \tau(z, s).
\end{aligned}$$

Use 1, above, to obtain the result.

3. The quantity (u, v) defined by:

$$(u, v) = (x, sy) \ominus \tau(x, sy) = \left(\left(\frac{\frac{s}{z^2}\tilde{y} - sy}{\tilde{x} - x}\right)^2 - \delta - \tilde{x} - x, -\frac{\frac{s}{z^2}\tilde{y} - sy}{\tilde{x} - x}u - \frac{sy\tilde{x} - \frac{s}{z^2}x\tilde{y}}{\tilde{x} - x}\right)$$

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 τ.

◇

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

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

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:

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

By Lemma 8.19 (3), we have:

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

Then, by the definition of τ, for any $(z_0, s_0) \in \mathcal{E}(\mathbf{C}_p) - \{\infty\}$, $z_0 \neq 0$, we have $\bar{x}(z_0^{-1}) = \bar{x}(z_0)$ and $-\frac{s_0}{z_0^2}\bar{y}(z_0^{-1}) = -s_0\bar{y}(z_0)$, that is $\bar{y}(z_0^{-1}) = z_0^2\bar{y}(z_0)$. The latter implies that the function $z\bar{y}$ is invariant under $z \mapsto z^{-1}$. We then apply Corollary 8.16 to the pair $(\bar{x}, z\bar{y})$ to conclude. ◇

Definition 8.21 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. $(x, sy) = 2(a, sb) \oplus (z, s)$). Further, we will say 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:

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

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

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

Lemma 8.22 *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 three points of order 2 are $(0, 0)$, $(\xi, 0)$ and $(\xi^{-1}, 0)$. Say that (a, b) is a solution of Equation (MD) over $\mathcal{M}_p$ such that $2(a, sb)$ is a point of order 2. Then

$$\frac{(a^2 - 1)^2}{4(\cdot F(a)}$$

is a constant, which implies that a is a constant (a is one of the roots of some non-trivial polynomial over $\mathbf{C}_p$). So $(sb)^2 = F(z)b^2$ is a constant. But this cannot be because $F(z)$ is not a square in $\mathcal{M}_p$ (F has been chosen so that it has three distinct zeros). We conclude that the points of order 2 are not even solutions.

Suppose now that there exists a solution both even and odd. It implies that (z, s) is even, that is, can be written as $2(a, sb)$. Then we have

$$\frac{(a^2 - 1)^2}{4 \cdot F(a)} = \frac{(a^2 - 1)^2}{4 \cdot F(z)b^2} = z,$$

which implies that $zF(z) = z^2(z^2 + \delta z + 1)$ is a square. This is absurd because we have chosen $\delta \neq \pm 2$. ◇

The next Corollary is not necessary for proving Theorem 8.24. We present it nevertheless because it gives a nice correspondence between two kinds of properties of the solutions of Equation (MD).

Corollary 8.23 *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 8.19 (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 8.20 would be even, which is impossible by Lemma 8.22. Then we are in the case $(x, sy) = \pm\tau(x, sy)$. From this equality, we obtain that the pair (x, sy) has the even property just by the definition of τ.

If $(x, sy) = 2(a, sb) \oplus (z, s)$, then by Lemma 8.19 (2), $\tau(x, sy) = 2\tau(a, sb) \oplus \tau(z, s)$, and it follows that:

$$\begin{aligned}(\bar{x}, s\bar{y}) &= 2(a, sb) \ominus \tau(2(a, sb)) \oplus (z, s) \ominus \tau(z, s)\\ &= (z, s) \ominus [(z, s) \oplus (0, 0)]\\ &= (0, 0)\end{aligned}$$

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

Theorem 8.24 *The solutions (x, y) of Equation (MD) over the field $\mathcal{M}_p$ of global meromorphic functions are rational.*

Proof: Assume that (x, y) is a solution of Equation (MD), x and y being functions in $\mathcal{M}_p$. By Lemma 8.20, the pair $(x \circ z^{-1}, -\frac{s}{z^2}(y \circ z^{-1})) \in \mathcal{E}(\mathcal{M}_p^*)$ can only be one of the following:

1. $\pm(x, sy)$.
2. $(x, sy) \oplus (0, 0)$, that is, $(\frac{1}{x}, -\frac{sy}{x^2})$.
3. $(x, sy) \oplus (\xi, 0)$ or $(x, sy) \oplus (\xi^{-1}, 0)$.

In Case 1 and Case 2 we have respectively $x(z^{-1}) = x(z)$ and $x(z^{-1}) = \frac{1}{x(z)}$. By Lemma 8.7, this implies that x, in both cases, is rational. For the third case, note that x cannot be equal to ξ because we would have $(\xi, 0) = 2(\xi, 0)$. Then the addition formula on $\mathcal{E}$ gives the following:

$$(x \circ z^{-1}, -\frac{s}{z^2}(y \circ z^{-1})) = (x, sy) \oplus (\xi, 0) = \left(\frac{\xi}{x}\left(\frac{sy}{x - \xi}\right)^2, -\frac{sy}{x - \xi}(\tilde{x} - \xi)\right),$$

where $\tilde{x} = x \circ z^{-1}$. Then we have:

$$x \circ z^{-1} = \frac{\xi}{x}\left(\frac{sy}{x - \xi}\right)^2,$$

which, since we have $(sy)^2 = x(x - \xi)(x - \xi^{-1})$, implies that:

$$x \circ z^{-1} = \xi\frac{x - \xi^{-1}}{x - \xi}.$$

Subtracting ξ from both sides, we obtain:

$$x \circ z^{-1} - \xi = \frac{\xi^2 - 1}{x - \xi}.$$

If we write $X = x - \xi$, we have

$$X(z^{-1}) = (\xi^2 - 1) \cdot \frac{1}{X(z)}.$$

By Lemma 8.7, the function X is then a rational function. This finishes the proof of the theorem. ◇

8.5 Analytic projective maps from an elliptic curve $\mathcal{E}$ minus the origin to $\mathcal{E}$

We will prove that Theorems 8.24 and 7.1, together, give a complete characterization of all the analytic projective maps from $\mathcal{E}$ minus a point to $\mathcal{E}$. First, we have to explain what we mean by *analytic projective map from $\mathcal{E}$ minus a point to $\mathcal{E}$.*

An *analytic function f on $\mathbf{C}_p^2$* is a function defined on $\mathbf{C}_p^2$ which admits a power series expansion on $\mathbf{C}_p^2$, i.e. (the indices n, m being non-negative) : there exists a formal power series

$$F = \sum_{\substack{k\geq 0\\ n+m=k}} a_{n,m}T^nU^m \in \mathbf{C}_p[[T,U]]$$

which converges for any values of T and U in $\mathbf{C}_p$ such that

$$\forall (z,w)\in \mathbf{C}_p^2, \quad f(z,w) = \sum_{\substack{k\geq 0\\ n+m=k}} a_{n,m}z^nw^m.$$

A *meromorphic function* on $\mathbf{C}_p^2$ is the quotient of two analytic functions on $\mathbf{C}_p^2$. By $\mathcal{A}_p(z)$ and $\mathcal{M}_p(z)$ we denote respectively the ring of global analytic functions and the field of global meromorphic functions of the variable z. We denote by $\mathcal{A}_p(z,w)$ the ring of analytic functions on $\mathbf{C}_p^2$ and by $\mathcal{M}_p(z,w)$ the field of meromorphic functions on $\mathbf{C}_p^2$, in the variable (z,w).

Let $\mathcal{E}$ be the elliptic curve defined by the affine equation

$$w^2 = z^3 + \delta z^2 + z.$$

Let $\sim$ denote the equivalence relation on $\mathcal{A}_p(z,w)$ and $\mathcal{M}_p(z,w)$ defined by : $f(z,w)\sim g(z,w)$ if and only if, for all $(z,w)\in \mathbf{C}_p^2$ such that whenever $w^2 = z^3+\delta z^2+z$, we have $f(z,w) = g(z,w)$. Let $\mathcal{A}_p(\mathcal{E}) = \mathcal{A}_p(z,w)/\sim$ and $\mathcal{M}_p(\mathcal{E}) = \mathcal{M}_p(z,w)/\sim$. An element of $\mathcal{A}_p(\mathcal{E})$ is called an *analytic function on $\mathcal{E}$* and an element of $\mathcal{M}_p(\mathcal{E})$ is called a *meromorphic function on $\mathcal{E}$.* Let s be an element in an algebraic closure of $\mathcal{M}_p(z)$ 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 $\mathcal{M}_p(z)$. Hence s is an element of degree 2 over $\mathcal{M}_p(z)$ and integral over $\mathcal{A}_p(z)$.
- We may identify $\mathcal{A}_p(\mathcal{E})$ with the ring $\mathcal{A}_p(z)[s]$ and $\mathcal{M}_p(\mathcal{E})$ with the field $\mathcal{M}_p(z)[s]$.

Definition 8.25 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 $\mathcal{A}_p(\mathcal{E})$, not all identically zero, such that

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

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

Let $P\in\mathcal{E}$ and $(z_P, s_P) = (z,s)\ominus P$. 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 $(\frac{g_1}{g_3},\frac{g_2}{g_3})$.

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 $\mathcal{M}_p(z)$. 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 $\mathbf{C}_p(z)$).

Lemma 8.26 *A function in $\mathcal{M}_p(z)$ which is algebraic over $\mathbf{C}_p(z)$ is a rational function.*

Proof: Let $f \in \mathcal{M}_p(z)$ and $P \in \mathbf{C}_p(z)[T]$ be a polynomial such that $P(f) = 0$.

Assume first that $f \in \mathcal{A}_p$. Without loss of generality, we can assume that P lies in $\mathbf{C}_p[z][T]$. Write $P(T) = \sum_{k=0}^n a_k T^k \in \mathbf{C}_p[z][T]$. So we have

$$f \cdot \left(\sum_{k=1}^n a_k f^{k-1} \right) = -a_0 \in \mathbf{C}_p[z].$$

Then it is obvious that f must be a polynomial, because f cannot have infinitely many zeros.

Suppose now that f lies in $\mathcal{M}_p(z)$ and is not rational. Without loss of generality, we can assume that P is a monic polynomial. If f has finitely many poles, there exists a polynomial $Q \in \mathbf{C}_p[z]$ such that fQ lies in $\mathcal{A}_p$. If the polynomial P has degree n, consider the polynomial $P_0 = Q^n(z)P$; we still have $P_0(f) = \sum_{k=0}^n a_k Q^{n-k}(fQ)^k = 0$. We deduce that fQ is a polynomial, which contradicts the non-rationality of f. Therefore f must have infinitely many poles. So there exists a pole ρ of f which is not a pole of the coefficients of P (since those coefficients are rational, they can have only finitely many zeros). Since P is a monic polynomial, ρ is a pole of $P(f)$. This contradicts the fact that $P(f) = 0$. $\diamond$

Theorem 8.27 *Let $P \in \mathcal{E}$. Any analytic projective map on $\mathcal{E} - \{P\}$ and into $\mathcal{E}$ is rational.*

Proof: 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 ∞. Write $G^+ = (a^+, b^+)$ and $G^- = (a^-, b^-)$. It is clear from the addition formula that a^+, b^+, a^- and b^- lie in $\mathcal{M}_p(\mathcal{E})$, and that the maps $G^+ = (a^+, b^+)$ and $G^- = (a^-, b^-)$ can be written as $G^+ = (a_0^+ + s a_1^+, b_0^+ + s b_1^+)$ and $G^- = (a_0^- + s a_1^-, b_0^- + s b_1^-)$. Moreover we have:

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

which implies that:

- If G^+ is not ∞, then $a_1^+ = b_1^+ = 0$, that is, $G^+ = (a_0^+, b_0^+)$ and then depends only on z.
- If G^- is not ∞, then $a_1^- = b_0^- = 0$, that is, $G^- = (a_0^-, s b_1^-)$.

By Theorem 7.1, G^+ is a constant. Moreover, the coordinates of G^- satisfy:

$$(s b_1^-)^2 = (a_0^-)^3 + \delta (a_0^-)^2 + a_0^-,$$

and then

$$(z^3 + \delta z^2 + z)(b_1^-)^2 = (a_0^-)^3 + \delta (a_0^-)^2 + a_0^-.$$

Therefore, (a_0^-, b_1^-) is a solution of Equation (MD) over $\mathcal{M}_p(z)$. By Theorem 8.24, 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

$$\frac{(u^2-1)^2}{4F(u)} = a \in \mathbf{C}_p(z,s).$$

Observe that $\mathbf{C}_p(z,s)$ is an algebraic extension of degree 2 of $\mathbf{C}_p(z)$ and then u is algebraic over $\mathbf{C}_p(z)$. Write $u = u_0 + su_1$ and $\bar{u} = u_0 - su_1$, where u_0 and u_1 are functions in $\mathcal{M}_p(z)$. It is clear that $\bar{u}$ is algebraic over $\mathbf{C}_p(z)$, therefore $u + \bar{u} = 2u_0$ and $u - \bar{u} = 2su_1$ are algebraic over $\mathbf{C}_p(z)$. So u_0 and u_1 are both algebraic over $\mathbf{C}_p(z)$. By Lemma 8.26, 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 ∞ is similar. ◇

8.6 Applications to definability and undecidability results - an analogue of Hilbert's tenth problem

What remains to be proved in order to prove the main theorem 1.2, follows by techniques by J. Denef in [11].

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 $\mathbf{C}_p(z)$ and the point $(z,1)$ is a point of $\mathcal{E}^*$. For any $n \neq 0$ in the ring $\mathrm{End}\,(\mathcal{E})$ 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 $\mathcal{E}$. More precisely, we have:

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

and the bijection $g\colon (x,y) \mapsto (x,sy)$ is additive, that is, denoting by $\overset{*}{\oplus}$ the addition law on $\mathcal{E}^*$,

$$g((x_1,y_1) \overset{*}{\oplus} (x_2,y_2)) = g(x_1,y_1) \oplus g(x_2,y_2).$$

We could have defined (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 $\mathbf{C}_p(z)$.

Lemma 8.28 *We have*

$$\frac{x_2'}{y_2} = 2.$$

Proof: This is clear by the addition formula. ◇

Lemma 8.29 *The function $\frac{x_n'}{y_n}$ is a constant function.*

Proof: On the one hand, we have

$$(x_{2n}, sy_{2n}) = 2n(z,s) = 2(x_n, sy_n) = (x_2 \circ x_n, sy_n \cdot y_2 \circ x_n),$$

which implies that

$$\frac{x_{2n}'}{y_{2n}} = \frac{(x_2 \circ x_n)'}{y_n \cdot y_2 \circ x_n} = \frac{x_n'}{y_n} \cdot \frac{x_2' \circ x_n}{y_2 \circ x_n} = 2\frac{x_n'}{y_n}.$$

On the other hand, we have

$$(x_{2n}, sy_{2n}) = 2n(z,s) = n(x_2, sy_2) = (x_n \circ x_2, sy_2 \cdot y_n \circ x_2),$$

which implies that

$$\frac{x_{2n}'}{y_{2n}} = \frac{(x_n \circ x_2)'}{y_2 \cdot y_n \circ x_2} = \frac{x_2'}{y_2} \cdot \frac{x_n' \circ x_2}{y_n \circ x_2} = 2\frac{x_n'}{y_n} \circ x_2.$$

Therefore we have

$$\frac{x_n'}{y_n} = \frac{x_n'}{y_n} \circ x_2.$$

Since x_2 is not the identity, it is clear that $\frac{x_n'}{y_n}$ has to be a constant function. ◇

Recall that P denotes the Weierstrass Laurent series of $\mathcal{E}$ (see section 7.1). We have the following corollary of Lemma 7.9.

Corollary 8.30 *We have*

$$\frac{x_n'}{y_n} \circ P = n.$$

Proof: From Lemma 7.9, we know that:

$$n(P, P') = (P, P') \circ (n\mathrm{Id}).$$

We have also, by definition of x_n and y_n:

$$n(P, P') = (x_n \circ P, P' \cdot y_n \circ P).$$

Therefore we obtain:

$$\begin{aligned} \frac{x_n'}{y_n} \circ P &= \frac{(x_n \circ P)'}{P' \cdot y_n \circ P} \\ &= \frac{(P \circ (n\mathrm{Id}))'}{P' \circ (n\mathrm{Id})} \\ &= n \end{aligned}$$

◇

Corollary 8.31 *For $n \in \mathrm{End}\,(\mathcal{E}) - \{0\}$, we have*

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

Proof: It follows from Lemma 8.29 and Corollary 8.30. ◇

Corollary 8.32 *For $n \in \mathrm{End}\,(\mathcal{E}) - \{0\}$, the order of x_n at 0 is equal either to 1 or to -1 and $\mathrm{ord}_0(y_n) = \mathrm{ord}_0(x_n) - 1$. Moreover, for $n \in \mathrm{End}\,(\mathcal{E}) - \{0\}$, we have*

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

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 Corollary 8.31 we have

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

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

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

If $\mathrm{ord}_0(x_n) > 0$, we find $\mathrm{ord}_0(y_n) = 0$ and $\mathrm{ord}_0(x_n) = 1$. While if $\mathrm{ord}_0(x_n) < 0$, we find $\mathrm{ord}_0(y_n) = -2$ and $\mathrm{ord}_0(x_n) = -1$. We conclude by Corollary 8.31. If $\mathrm{ord}_0(x_n) = 1$, we obtain $\frac{x_n}{zy_n}|_{z=0} = n$, and if $\mathrm{ord}_0(x_n) = -1$, we obtain $\frac{x_n}{zy_n}|_{z=0} = -n$. ◇

Corollary 8.33 *For $n \in \mathrm{End}(\mathcal{E}) - \{0\}$, 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 $\mathrm{ord}_0(x_1) = 1$. From the duplication formula, we get

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

therefore we have $\mathrm{ord}_0(x_2) = -1$. 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 8.32, we have only two cases: either $\mathrm{ord}_0(x_n) = 1$ or $\mathrm{ord}_0(x_n) = -1$. In both cases, one can see that $\mathrm{ord}_0(x_{2n}) = -1$.

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

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

We write

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

Since $\mathrm{ord}_0(x_{2n}) = -1$, we have, by Corollary 8.32, $\mathrm{ord}_0(y_n) = -2$. We know also by Corollary 8.32 that $\frac{x_{2n}}{zy_{2n}}|_{z=0} = -n$. Therefore we obtain

$$\mathrm{ord}_0\left(\frac{zy_n-x_n}{z-x_n}\right) = 0$$

which implies that

$$\mathrm{ord}_0(x_{n+1}) = \mathrm{ord}_0(z^3+\delta z^2+z) - \mathrm{ord}_0(zx_n).$$

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

For the next lemma, one can look in [11, part 3], or in [41].

Lemma 8.34 *[Denef]*

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 $\{(x_n, y_n) \mid n \in \mathrm{End}(\mathcal{E})\}$ is existentially definable in the field of rational functions $\mathbf{C}_p(z)$.*

Proof of Main Theorem 1.2:

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

$$\mu = 0 \vee \exists x, y, a, b, v, w\, [F(z)b^2 = F(a) \wedge (x, y) = 2(a, b) \wedge y \neq 0 \\ \wedge vzy = x \wedge \mathrm{ord}_0(v + 2\mu) > 0 \wedge w^2 = F(2\mu)].$$

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

Let $\mu \in \mathcal{M}_p - \{0\}$, such that the formula $\varphi(\mu)$ is true in $\mathcal{M}_p$. Then there exist $a, b, x, y \in \mathcal{M}_p$ such that (a, b) and $(x, y) = 2(a, b)$ satisfy Equation (MD). By Theorem 8.24, they must be rational. By Lemma 8.34 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 8.22), it is clear that the integer m must be even; say $m = 2n$. Set $v \in \mathcal{M}_p$ such that $v = \frac{x}{zy}$. From Corollaries 8.32 and 8.33, we deduce that $v(0) = -2n$. Since we have $\mathrm{ord}_0(v + 2\mu) > 0$, the function -2μ 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 Theorem 7.1 that the function μ must be constant. So $\mu = n$.

Let us prove the converse. Suppose $\mu = n$ is a non-zero integer. Choose $x = x_{2n}$, $y = y_{2n}$, $a = x_n$, $b = y_n$, $v = \frac{x_{2n}}{zy_{2n}}$ and w such that $w^2 = F(2n)$. Using the properties of (x_n, y_n) (see Corollaries 8.32 and 8.33), it is easy to see that the formula $\varphi(\mu)$ is satisfied. ◇

The following corollary was proved in [32].

Corollary 8.35 (Lipshitz-Pheidas) *The positive existential theory of the ring $\mathcal{A}_p$ of global analytic functions, in the language $\mathcal{L}_R^z$, is undecidable.*

Proof: We represent each meromorphic function x of $\mathcal{M}_p$ as the quotient of two analytic functions, $x = \frac{x_1}{x_2}$, with $x_1, x_2 \in \mathcal{A}_p$ and $x_2 \neq 0$; note that, by Theorem 7.1, if $c \in \mathcal{A}_p$ then $c \in \mathbf{C}_p$ if and only if there exists a $d \in \mathcal{A}_p$ such that $c^2 = d^3 + d^2 + d$; and $c \in \mathbf{C}_p$ is non-zero if and only if there exists $d \in \mathbf{C}_p$ such that $cd = 1$. Also $\mathrm{ord}_0(x)$ is greater than 0 if and only if the following holds:

"There exists $c \in \mathbf{C}_p^*$ such that z divides $x_2 - c$ and z divides x_1." (division is understood in $\mathcal{A}_p$)

It is then obvious that every existential formula of $\mathcal{L}_R^*$ over $\mathcal{M}_p$ is equivalent to an existential formula over $\mathcal{A}_p$. Finally note that if $x_2 \in \mathcal{A}_p$, then $x_2 \neq 0$ if and only if there exist $c, e, f \in \mathbf{C}_p$ such that $ef = 1$ and $z - c$ divides $x_2 - e$ in $\mathcal{A}_p$. Therefore every existential formula of $\mathcal{L}_R^z$ over $\mathcal{A}_p$ is equivalent to a positive existential formula of $\mathcal{L}_R^z$. Hence the result follows. ◇

References

[1] Y. Amice, *Les nombres p-adiques*, Presses Universitaires de France, Coll. Sup. (1975).

[2] J. Ax, S. Kochen, *Diophantine problems over local fields: III Decidable fields*, Ann. Math. **83** (1966), 437-456.

[3] L. Becker, C. W. Henson, L. A. Rubel, *First order conformal invariants*, Ann. Math. (2) **112** (1980), 123-178.

[4] W. Berkovich, *Spectral theory and analytic geometry over non-archimedian fields*, Math. surveys and monographs, Coll. Amer. Math. Soc. (1990).

[5] A. Boutabaa, A. Escassut, *Applications of the p-adic Nevanlinna theory to functional equations*, to appear in Annales de l'Institut Fourier (2001).

[6] C. C. Chang, *Model theory*, North Holl. Publish. Company, Coll. Stud. in Logic and Found. of Math. (1990).

[7] R. Cori, D. Lascar, *Logique mathématique*, Masson, Coll. Axiomes (1996).

[8] M. Davis, *Hilbert's tenth problem is unsolvable*, American Mathematical Monthly **80** (1973), 233-269.

[9] F. Delon, *Indécidabilité de la théorie des anneaux de séries formelles à plusieurs variables*, Fund. Math. CXII (1981), 215-229.

[10] J. Denef, *Hilbert's tenth problem for quadratic rings*, Proc. Amer. Math. Soc. **48** (1975), 214-220.

[11] J. Denef, *The diophantine problem for polynomial rings and fields of rational functions*, Trans. Amer. Math. Soc. **242** (1978).

[12] J. Denef, *The Diophantine problem for polynomial rings of positive characteristic*, Logic Colloquium **78**, North Holland (1984), 131-145.

[13] J. Denef, *p-adic semi-algebraic sets and cell decomposition*, J. Reine Angew. Math. **369** (1986), 154-166.

[14] J. Denef, L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, Jour. Lond. Math. Soc. (2) **18** (1978), 385-391.

[15] J. Denef, L. Lipshitz, *Power series solutions of algebraic differential equations*, Math. Ann. **267** (1980), 1-28.

[16] J. Denef, M. Gromov, *The ring of analytic functions in the disk has undecidable theory*, (1985), letter.

[17] J. Denef, L. van den Dries, *p-adic and real subanalytic sets*, Ann. Math. **128** (1988), 79-138.

[18] J.-L. Duret, *Sur la théorie élémentaire des corps de fonctions*, Journ. Symb. Logic **51**, n4 (1986), 948-956.

[19] J.-L. Duret, *Équivalence élémentaire et isomorphisme des corps de courbe sur un corps algébriquement clos*, Journ. Symb. Logic **57**, n3 (1992), 808-823.

[20] P. Du Val, *Elliptic Functions and elliptic curves*, Lond. Math. Soc. Lect. Note Series **9**, Cambridge University Press (1973).

[21] L. van den Dries, *A specialization theorem for analytic functions on compact sets*, Nederl. Akad. Wetensch. Indag. Math. **44** (1982), 391-396.

[22] L. van den Dries, *A specialization theorem for p-adic power series which converge on the closed unit disk*, Jour. Alg. **73** (1981), 613-623.

[23] Y. Eršov, *On the elementary theory of maximal normed fields*, Dokl. Akad. Nauk. SSSR **165** (1965), 1390-1393.

[24] A. Escassut, *Analytic elements in p-adic analysis*, World Scientific (1995).

[25] F. Q. Gouvêa, *p-Adic numbers, an introduction*, Springer-Verlag (1993).

[26] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New-York (1977).

[27] S. Kochen, *The model theory of local fields*, Lecture Notes in Math. **499** (1975), 384-425.

[28] S. Lang, *Elliptic functions, 2nd edition*, Springer Verlag, Grad. Texts in Math. (1987).

[29] S. Lang, *Complex analysis, 4th edition*, Springer Verlag, Grad. Texts in Math. (1999).

[30] M. Lazard, *Les zros d'une fonction analytique d'une variable*, I. H. E. S. **14** (1962), 47-75.

[31] L. Lipshitz, *The Diophantine problem for addition and divisibility*, Trans. Amer. Math. Soc. **235** (1978), 271-283.

[32] L. Lipshitz, A. Pheidas, *An analogue of Hilbert's tenth problem for p-adic entire functions*, Jour. Symb. Logic **60**, N. 4 (1995).

[33] A. Macintyre, *On definable subsets of p-adic fields*, Jour. Symb. Logic **41** (1976), 605-610.

[34] Y. Matiyasevich, (or Matijasevich, or Matiiasevich) *Enumerable sets are diophantine*, Dkl. Akad. Nauk. SSSR **191** (1970), 279-282. English translation Soviet. Math Dokl. **11** (1970), 354-358.

[35] Y. Matiiasevich, *Le dixième problème de Hilbert et son indécidabilité* Paris Milan Barcelone Masson (1995).

[36] A. F. Monna, *Analyse non-archimdienne* Springer Verlag, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 56 (1970).

[37] D. A. Pierce, *Function fields and elementary equivalence*, Bull. Lond. Math. Soc. **31**, 4 (1999).

[38] A. Pheidas, *Hilbert's tenth problem for fields of rational functions over finite fields*, Inv. Math. **103** (1991), 1-8.

[39] A. Pheidas, *Extensions of Hilbert's tenth problem*, Jour. Symb. Logic **59**, N. 2 (1994).

[40] A. Pheidas, *The Diophantine theory of a ring of analytic functions*, J. Reine Angew. Math. **463** (1995), 153-157.

[41] A. Pheidas, K. Zahidi *Undecidability of existential theories of rings and fields: a survey*, Contemp. Math. **270** (2001), 49-106.

[42] A. M. Robert, *A course in p-adic analysis*, Springer-Verlag, Grad. texts in math. (2000).

[43] J. Robinson, *Definability and decision problems in arithmetic*, Jour. Symb. Logic **14** (1949), 98-114.

[44] R. Robinson, *Undecidable rings*, Trans. Amer. Math. Soc. **70** (1951), 137.

[45] L. Rubel, *An essay on Diophantine equations for analytic functions*, Exp. Math. **13** (1995), 81-92.

[46] J. H. Silverman, *The arithmetic of elliptic curves*, Springer Verlag, Grad. texts in math. (1986).

[47] X. Vidaux, *Équivalence élémentaire de corps elliptiques*, C. R. Acad. Sci. Paris, Série I **330**, (2000), 1-4.

[48] K. Zahidi, *The existential theory of real hyperelliptic function fields*, To appear in Jour. Algebra.

[49] K. Zahidi, *Existential undecidability for rings of algebraic functions*, Ph.D thesis, University of Ghent (1999).

Université d'Angers,
Département de Mathématiques,
2 Bd Lavoisier,
49045 Angers
France

University of Crete-Heraklion,
Department of Mathematics,
71 409 Heraklion,
Crete-Greece

Xavier.Vidaux@univ-angers.fr
vidaux@math.itia.uch.gr

Dans la première partie, nous démontrons une partie d'une conjecture de J.-L. Duret. Soit k un corps algébriquement clos de cartactéristique zéro et K et K' deux corps elliptiques sur k. Supposons que K est avec multiplication complexe et soit j son invariant modulaire. Soit $\mathcal{L}_R(j)$ le langage des corps enrichi d'un symbole de constante pour j. Soient $\mathcal{E}$ et $\mathcal{E}'$ des courbes ayant pour corps de fonctions respectivement K et K'. Nous démontrons que si les corps K et K' sont élémentairement équivalents dans le langage $\mathcal{L}_R(j)$, alors les courbes $\mathcal{E}$ et $\mathcal{E}'$ ont des anneaux d'endomorphismes isomorphes.

La seconde partie est consacrée à l'étude d'un analogue du dixième problème de Hilbert (existence ou non d'un algorithme qui décide, pour une équation diophantienne quelconque, si l'équation a ou n'a pas de solutions dans les entiers). Y. Matiyasevich a répondu négativement au dixième problème de Hilbert en 1970. Soit $\mathcal{L}_R^*$ le langage des anneaux enrichi par un symbole de constante pour la variable z et d'un symbole de relation unaire $\ll \operatorname{ord}_0(x) > 0 \gg$ (la fonction x s'annule en 0). Nous démontrons que les entiers naturels sont définissables dans le corps $\mathcal{M}_p$ des fonctions méromorphes p-adiques globales, dans le langage $\mathcal{L}_R^*$. Il s'ensuit que la théorie existentielle du corps $\mathcal{M}_p$ dans le langage $\mathcal{L}_R^*$ est indécidable. Afin de démontrer ces théorèmes, nous obtenons : 1) une caractérisation des paramétrisations p-adiques méromorphes d'une courbe elliptique, définie sur le corps des constantes; 2) une caractérisation complète des fonctions méromorphes p-adiques d'une courbe elliptique $\mathcal{E}$ moins un point vers $\mathcal{E}$ (pour toute courbe elliptique définie sur le corps des constantes).

Elementary equivalence of elliptic fields - Hilbert's tenth problem for p-adic global meromorphic functions

In the first part, we prove a part of a conjecture of J.-L. Duret. Let k be an algebraically closed field of characteristic zero. Let K and K' be two elliptic fields over k. Assume that K has complex multiplication and modular invariant j. Let $\mathcal{L}_R(j)$ denote the language of fields augmented by a symbol of constant for j. Let $\mathcal{E}$ and $\mathcal{E}'$ be curves whose function fields are respectively K and K'. We prove that if the fields K and K' are elementarily equivalent in the language $\mathcal{L}_R(j)$, then the curves $\mathcal{E}$ and $\mathcal{E}'$ have isomorphic rings of endomorphisms.

The second part is dealing with an analogue of Hilbert's tenth problem (existence or not of an algorithm which decides, for any given Diophantine equation, whether the equation has or does not have integer solutions). Hilbert's tenth problem was answered negatively by Y. Matiyasevich in 1970. Let $\mathcal{L}_R^*$ be the language of rings augmented by a constant symbol for the variable z and by a symbol for the unary relation "$\operatorname{ord}_0(x) > 0$" (the function x takes the value 0 at 0). We prove that the set of rational integers is positive existentially definable in the field $\mathcal{M}_p$ of p-adic global meromorphic functions, in the language $\mathcal{L}_R^*$. Thus the positive existential theory of the field $\mathcal{M}_p$ in the language $\mathcal{L}_R^*$ is undecidable. In order to prove these theorems, we obtain : 1) a characterization of the p-adic meromorphic parametrizations of an elliptic curve, defined over the field of constants; 2) a complete characterization of all p-adic meromorphic maps from an elliptic curve $\mathcal{E}$ minus a point to $\mathcal{E}$ (for any elliptic curve defined over the field of constants).

Discipline : MATHÉMATIQUES - Spécialité : LOGIQUE

MOTS-CLES : logique, théorie des modèles, courbes elliptiques, équivalence élémentaire, dixième problème de Hilbert, analyse p-adique, fonctions méromorphes p-adiques, fonctions méromorphes sur courbes elliptiques affines

Département de Mathématiques, 2 Bd Lavoisier, 49045 Angers, France