ARITHMETIC DEFORMATION THEORY VIA ARITHMETIC FUNDAMENTAL GROUPS AND NONARCHIMEDEAN THETA-FUNCTIONS, NOTES ON THE WORK OF SHINICHI MOCHIZUKI

IVAN FESENKO

ABSTRACT. These notes survey the main ideas, concepts and objects of the work by Shinichi Mochizuki on *inter-universal Teichmüller theory* [31], which might also be called *arithmetic deformation theory*, and its application to diophantine geometry. They provide an external perspective which complements the review texts [32] and [33]. Some important developments which preceded [31] are presented in the first section. Several important aspects of arithmetic deformation theory are discussed in the second section. Its main theorem gives an inequality–bound on the size of volume deformation associated to a certain log-theta-lattice. The application to several fundamental conjectures in number theory follows from a further direct computation of the right hand side of the inequality. The third section considers additional related topics, including practical hints on how to study the theory.

This text is published in Europ. J. Math. (2015) 1:405–440.

CONTENTS

Foreword. The aim of these notes is to present, in a relatively simple form, the key ideas, concepts and objects of the work of Shinichi Mochizuki on inter-universal Teichmüller theory (IUT), to as many potential readers as possible. The presentation is based on my own experience in studying IUT. This text is expected to help its readers to gain a general overview of the theory and a certain orientation in it, as well as to see various links between it and existing theories.

Reading these notes cannot replace or substitute a serious study of IUT. As mentioned in [35], there are currently no shortcuts in the study of IUT. Hence there are probably two main options available at the time of writing of this text to learn about the essence of IUT. The first is to dedicate a significant amount of time[1] to studying the theory patiently and gradually reaching its main parts. I refer to section 3 for my personal advice on how to study the original texts of arithmetic deformation theory, which is another name (due to the author of the present text) for the theory. The second option is to read the review texts [32] and [33] and introductions of papers, etc. My experience and the experience of several other mathematicians show that the review texts could be hard to follow, and reading them before a serious study of IUT may be not the best way, while reading them after some preliminary study or in the middle of it can be more useful. We shall see to what extent this feature is shared by these notes.

In view of the declared aim of this text and the natural limitation on its size, it is inevitable that several important mathematical objects and notions in section 2 are introduced in a vague form such as a so-called theta-link: a very large part of [31]-I-III defines the theta-link and develops its enhanced versions.[2]

1. The origins

1.1. **From class field theory to reconstructing number fields to coverings of $\mathbb{P}^1$ minus three points.** Abelian *class field theory* for one-dimensional global and local fields, in particular for number fields and their completions, has played a central role in number theory and stimulated many further developments. Inverse Galois theory, several versions of the Langlands programme, anabelian geometry, (abelian) higher class field theory and higher adelic geometry and analysis, and, to some extent, the arithmetic of abelian varieties over global fields and their completions are among them.

Inverse Galois theory studies how to realise finite or infinite compact topological groups as Galois groups of various fields including extensions of number fields and their completions, see e.g. [21]. For abelian groups and local and global fields, the answer follows from class field theory. A theorem of Shafarevich states that every soluble group can be realised as a Galois group over a global field, see e.g. §6 Ch.IX of [40].

Let K^{alg} be an algebraic closure of a number field K. The Galois group $G_K = G(K^{\mathrm{alg}}/K)$ is called the absolute Galois group of K.

The *Neukirch–Ikeda–Uchida theorem* (proved by the end of 1970s; the proof used global class field theory) asserts, see e.g. §2 Ch.XII of [40], the following:

[1] in my opinion, at least 250–500 hours

[2] An appreciation of the general qualitative aspects of the theta-link may be obtained by studying the simplest version of the theta-link. This version is discussed in §I1 of [31]-I, while technical details concerning the construction of this version may be found in approximately 30 pages of §3 of [31]-I.

> For two number fields K_1, K_2 and any isomorphism of topological groups $\psi\colon G_{K_1} \xrightarrow{\sim} G_{K_2}$ there is a unique field isomorphism $\sigma\colon K_2^{\mathrm{alg}} \xrightarrow{\sim} K_1^{\mathrm{alg}}$ such that $\sigma(K_2) = K_1$ and $\psi(g)(a) = \sigma^{-1}(g\sigma(a))$ for all $a \in K_2^{\mathrm{alg}}$, $g \in G_{K_1}$. In particular, the homomorphism $G_{\mathbb{Q}} \to \mathrm{Aut}(G_{\mathbb{Q}})$, $g \mapsto (h \mapsto ghg^{-1})$, is an isomorphism and every automorphism of $G_{\mathbb{Q}}$ is inner.

The next theorem was included as Th. 4 in [3] in 1980, as part of Belyi's study of aspects of inverse Galois theory:

> An irreducible smooth projective algebraic curve C defined over a field of characteristic zero can be defined over an algebraic closure $\mathbb{Q}^{\mathrm{alg}}$ of the field of rational numbers $\mathbb{Q}$ if and only if there is a covering $C \longrightarrow \mathbb{P}^1$ which ramifies over no more than three points of $\mathbb{P}^1$.

This theorem[3] plays a key role in the study of Galois groups, including algebraic and geometric fundamental groups of curves over number fields and local fields.[4] Coverings of the type which appears in this theorem are often called *Belyi maps*. Various versions of Belyi maps are used in arithmetic deformation theory and its application to diophantine geometry.

1.2. **A development in diophantine geometry.** In 1983 Faltings proved the Mordell conjecture, a fundamental finiteness property in diophantine geometry [8], [2]. The *Faltings–Mordell theorem* asserts that

> A curve C of genus > 1 defined over an algebraic number field K has only finitely many rational points over K.

Several other proofs followed.[5] Vojta found interesting links with Nevanlinna theory in complex analysis which led to one of his proofs. For textbook expositions of simplified proofs see [15] and [6].

The same year Grothendieck wrote a letter [13] to Faltings, which proposed elements of *anabelian geometry*. With hindsight, one of the issues raised in it was a generalisation of the Neukirch–Ikeda–Uchida theorem[6] to anabelian geometric objects such as hyperbolic curves over number fields and possible applications of anabelian geometry to provide new proofs and stronger versions, as well as a better understanding, of such results in diophantine geometry as the Faltings–Mordell theorem, cf. 1.5.

---

[3] The first version of [3] and Belyi's seminar talk in Moscow dealt with an elliptic curve, which was enough for its subsequent application, see 1.5. After reading the first version of [3], Bogomolov noticed that the original proof of the theorem in it works for arbitrary curves. He told Belyi how important this extended version is and urged him to include the extended version in the paper. Belyi was reluctant to include the extended version, on the grounds that over finite fields every irreducible smooth projective algebraic curve may be exhibited as a covering of the projective line with at most one ramification point. Bogomolov then talked with Shafarevich, who immediately appreciated the value of the extended version and insisted that the author include it in [3]. Bogomolov further developed the theory of Belyi maps, in particular, in relation to the use of coloured Riemann surfaces and delivered numerous talks on these further developments. Several years later this theory appeared, independently, in Grothendieck's text [12].

[4] Grothendieck wrote about the "only if" part: "never, without a doubt, was such a deep and disconcerting result proved in so few lines!"[12].

[5] Here we are in the best possible situation when a conjecture stated over an arbitrary algebraic number field and is established over an arbitrary algebraic number field, and the methods of the proofs do not depend on the specific features of the number field under consideration. This is not so in the case of the arithmetic Langlands correspondence, even for elliptic curves over number fields. In the history of class field theory, the initial period of developing special theories that work only over small number fields was followed by a phase of general functorial class field theory over arbitrary global and local fields. The general theory was eventually clarified and simplified, see [39], and it became easier than those initial theories. We are yet to witness a similar phase which involves a general functorial theory that works over arbitrary number fields in the case of the Langlands programme and hence, in particular, yields another proof of the Wiles–Fermat theorem via the automorphic properties of elliptic curves over any number field.

[6] it appears that Grothendieck was not aware of this theorem

1.3. **Conjectural inequalities for the same property.** There are several closely related conjectures, proposed in the period from 1978 to 1987, which extend further the property stated in the Mordell conjecture:

(a) the *effective Mordell conjecture* — a conjectural extension of the Faltings–Mordell theorem which involves an effective bound on the height of rational points of the curve C over the number field K in the Faltings theorem in terms of data associated to C and K,
(b) the *Szpiro conjecture*, see below,
(c) the *Masser–Oesterlé conjecture*, a.k.a. the *abc conjecture* (whose statement over $\mathbb{Q}$ is well known[7], and which has an extension to arbitrary algebraic number fields, see Conj. 14.4.12 of [6]),
(d) the *Frey conjecture*, see Conj. F.3.2(b) of [15],
(e) the *Vojta conjecture* on hyperbolic curves, see below,
(f) *arithmetic Bogomolov–Miyaoka–Yau conjectures* (there are several versions).

The Szpiro conjecture was stated several years before[8] the work of Faltings, who learned much about the subject related to his proof from Szpiro. Using the Frey curve[9], it is not difficult to show that (c) and (d) are equivalent and that they imply (b), see e.g. see sect. F3 of [15] and references therein. Using Belyi maps as in 1.1, one can show the equivalence of (c) and (a). For the equivalence of (c) and (e) see e.g. Th. 14.4.16 of [6] and [47]. For implications (e) $\Rightarrow$ (f) see [48].

Over the complex numbers the property analogous to the Szpiro conjecture is very interesting. For a smooth projective surface equipped with a structure of non-split minimal elliptic surface fibred over a smooth projective connected complex curve of genus g, such that the fibration admits a global section, and, moreover, every singular fibre of the fibration is of type I_n, i.e. its components are projective lines which intersect transversally and form an n-gon, this property states that the sum of the number of components of singular fibres does not exceed 6 times the sum of the number of singular fibres and of $2g-2$. The property has several proofs, of which the first was given by Szpiro. Shioda deduced the statement in two pages of computations from arguments already known to Kodaira. These two proofs of the geometric version of the inequality use the cotangent bundle and the Kodaira–Spencer map. A (full) arithmetic version of the Kodaira–Spencer map could be quite useful for giving a proof of the arithmetic Szpiro conjecture. However, such an arithmetic version of the Kodaira–Spencer map is not yet known.

Among several other proofs of this property, a proof by Bogomolov uses monodromy actions and the hyperbolic geometry of the upper half-plane and does not use the cotangent bundle, see sect. 5.3 of [1]. His proof makes essential use of the fact that the n-gons determined by the singular fibres may be equipped with a common orientation, like windmills revolving in synchrony in the presence of wind. *Synchronisation* of data plays an important role in arithmetic deformation theory as well, cf. 2.10. To develop an arithmetic analogue of the geometric proof of Bogomolov to apply to proving the arithmetic Szpiro conjecture, one needs a kind of arithmetic analogue of the hyperbolic geometry of the upper half-plane, and this is in some sense achieved by IUT, see 2.10.

The conjectural (arithmetic) Szpiro inequality states in particular that if K is a number field, then for every $\varepsilon > 0$ there is a real c (depending on K and ε) such that for every elliptic curve E_K over the number field K

[7] For every $\varepsilon > 0$ there is a constant such that for all non-zero integers a,b,c such that $(a,b,c) = 1$ the equality $a+b+c = 0$ implies $\max(\log|a|, \log|b|, \log|c|) \leqslant \text{constant} + (1+\varepsilon)\sum_{p|abc} \log p$ where p runs through all positive primes dividing abc. While the statement of the abc conjecture does not reveal immediately any underlying geometric structure, the other conjectures are more geometrical. For an entertaining presentation of aspects of the abc conjecture and related properties, see e.g. [49].

[8] In 1978 Szpiro talked about it with several mathematicians. He made the conjecture public at a meeting of the German Math. Society (DMV) in 1982 where Frey, Oesterlé and Masser were present.

[9] $y^2 = x(x+a)(x-b)$ where $a, b, a+b$ are non-zero coprime integers

with split multiplicative reduction at every bad reduction valuation, so all singular fibres of its minimal regular proper model $\mathscr{E} \longrightarrow \operatorname{Spec} O_K$ are of type I_n, the weighted sum of the numbers n_v of components of singular fibres satisfies

$$\sum n_v \log|k(v)| \leqslant c + (6+\varepsilon)\sum \log|k(v)|,$$

where v runs through the nonarchimedean valuations[10] of K corresponding to singular fibres, and $k(v)$ denotes the finite residue field of K at v.[11] For the curve E_K as above, the quantity $\exp(\sum n_v \log|k(v)|)$ coincides with the absolute norm $N(\operatorname{Disc}_{E_K})$ of the so-called minimal discriminant of E_K, and $\exp(\sum \log|k(v)|)$ coincides with the absolute norm $N(\operatorname{Cond}_{E_K})$ of the conductor of E_K.[12] Using these notational conventions, the *Szpiro conjecture* states that if K is a number field, then for every $\varepsilon > 0$ there is a real $c' > 0$ (depending on K and ε) such that for every elliptic curve E_K over K the inequality

$$N(\operatorname{Disc}_{E_K}) \leqslant c' N(\operatorname{Cond}_{E_K})^{6+\varepsilon}$$

holds, see e.g. 10.6 of Ch.IV of [44].[13]

The *Vojta conjecture*, as discussed in this text, deals with a smooth proper geometrically connected curve C over a number field K and a reduced effective divisor D on C such that the line bundle $\omega_C(D)$, associated with the sum of the divisor D and a canonical divisor of C, is of positive degree (i.e. $C \setminus D$ is a hyperbolic curve, see 1.5). It asserts the following: for every positive integer n and positive real number ε there is a constant c (depending on C, D, n, ε but not on K) such that the inequality

$$\operatorname{ht}_{\omega_C(D)}(x) \leqslant c + (1+\varepsilon)(\text{log-diff}_C(x) + \text{log-cond}_D(x))$$

holds for all $x \in (C \setminus D)(K')$, for all number fields K' of degree $\leqslant n$. To define the terms, let $\mathscr{C}$ be a regular proper model of C over $\operatorname{Spec}(O_K)$. For a point $x \in C(\mathbb{Q}^{\mathrm{alg}})$ denote by F a minimal subfield of $\mathbb{Q}^{\mathrm{alg}}$ over which x is defined. Let $s_x \colon \operatorname{Spec}(O_F) \longrightarrow \mathscr{C}$ be the section uniquely determined by x. Then the height of x associated to a line bundle B on C can be explicitly defined in several equivalent ways (up to a bounded function on $C(\mathbb{Q}^{\mathrm{alg}})$), for instance, by using the canonical height on some projective space into which C is embedded, or as $\deg(s_x^* \mathscr{B})$, where $\mathscr{B}$ is an extension to $\mathscr{C}$ of B viewed as an arithmetic line bundle on C, cf. sect. 1 of [29] or part B of [15]. Define $\text{log-cond}_D(x) = \deg((s_x^* \mathscr{D})_{\mathrm{red}})$, where $\mathscr{D}$ denotes the closure in $\mathscr{C}$ of D, and red stands for the reduced part. Define $\text{log-diff}_C(x) = \deg(\delta_{F/\mathbb{Q}}) = |F:\mathbb{Q}|^{-1} \deg(D_{F/\mathbb{Q}})$ where $\delta_{F/\mathbb{Q}}$ and $D_{F/\mathbb{Q}}$ are the different and discriminant of $F/\mathbb{Q}$, and the normalised degree deg is defined in 2.2.[14] This conjecture is equivalent to Conj. 2.3 for curves in [47] or Conj. 14.4.10 in [6].

Using the Belyi map, one reduces the Vojta conjecture for C, D, K as above to the case of $C = \mathbb{P}^1$ over $\mathbb{Q}$ and $D = [0] + [1] + [\infty]$.[15]

---

[10] by abuse of some of the established terminology, valuations in this text include nonarchimedean and archimedean ones

[11] the notation $|J|$ stands for the cardinality of the set J

[12] there are two different objects in this text (and in this subsection) whose names involve the word "discriminant": the minimal discriminant $\operatorname{Disc}_{E_K}$ of an elliptic curve E_K over a number field K and the (absolute) discriminant $D_{K/\mathbb{Q}}$ of a number field K

[13] Szpiro proved that over $\mathbb{Q}$ this inequality implies the abc conjecture over $\mathbb{Q}$ with constant $6/5$ instead of constant 1 in it, see e.g. p.598 of [15].

[14] for a field extension R/S the notation $|R:S|$ stands for its degree

[15] Viewing $\mathbb{P}^1$ as the λ-line in the Legendre representation $y^2 = x(x-1)(x-\lambda)$ of an elliptic curve E_λ yields a classifying morphism from $\mathbb{P}^1 \setminus \{0,1,\infty\}$ to the natural compactification $M_{\mathrm{ell}} \otimes \mathbb{Q}$ of the moduli stack of elliptic curves over $\mathbb{Z}$ tensored with $\mathbb{Q}$. The height $\operatorname{ht}_{\omega_C(D)}(\lambda)$ on the LHS of the Vojta conjecture for $C = \mathbb{P}^1$ and $D = [0]+[1]+[\infty]$, is closely related to $\frac{1}{6}$ times the LHS of the inequality of the Szpiro conjecture for E_λ, since the degree of the pull-back to $\mathbb{P}^1$ of the divisor at infinity of the natural compactification of $M_{\mathrm{ell}} \otimes \mathbb{Q}$ is 6 times 1 = the degree of $\omega_C(D)$, see [29].

Note the difference between the Vojta conjecture and the Szpiro conjecture in relation to allowing the algebraic number field to vary; this partially explains the occurrence of the term involving log-diff$_C$ on the RHS of the inequality of the former conjecture. One can formulate a stronger version of the Szpiro conjecture in which K varies.[16] The Frey conjecture, the Szpiro conjecture and the stronger Szpiro conjecture are problems in arithmetic of elliptic curves over number fields. There are three basic methods to work on fundamental problems in arithmetic of elliptic curves: (i) the more traditional use of Galois groups generated by certain torsion points of the elliptic curve E_K and associated Galois representations, in particular, this is how the Wiles–Fermat theorem was proved, (ii) the method of IUT which involves the arithmetic fundamental group of hyperbolic curves over number fields related to the elliptic curve E_K, among several ingredients, (iii) higher adelic method uses the abelian part of the absolute Galois group of the function field of the elliptic curve E_K, two-dimensional class field theory, higher adeles and higher zeta integrals, [9] and 2.14.

There are also so-called explicit stronger versions of the abc conjecture, which easily imply the Wiles–Fermat theorem, see e.g. [49], and which are not dealt with in [31]. For a discussion of the relationship between [31] and solutions to the Fermat equation see the final paragraph of 2.12.

1.4. **A question posed to a student by his thesis advisor.** In January 1991 Shinichi Mochizuki, at that time a third year PhD student in Princeton, 21 years old, was asked by Faltings (his thesis advisor) to try to prove the effective form of the Mordell conjecture.[17]

Not surprisingly, he was not able to prove it during his PhD years. As we know, he took the request of his supervisor very seriously. In hindsight, it is astounding that almost all his papers are related to the ultimate goal of establishing the conjectures of 1.3. These efforts over the long term culminated twenty years later in [31]-IV, where (a), (c), (d), (e) and hence (b) and (f) of 1.3 are established as one application of his inter-universal Teichmüller theory [31]-I-III.[18]

His earlier Hodge–Arakelov theory [23], where a certain weak arithmetic version of the Kodaira–Spencer map is studied, was already an innovative step forward. That work shows that Galois groups may in some sense be regarded as arithmetic tangent bundles.

1.5. **On anabelian geometry.** *Algebraic (or étale) fundamental groups* in general and anabelian geometry in particular are less familiar to number theorists than class field theory or parts of diophantine geometry. On the other hand, geometers may feel more at home in this context. For an introduction to many relevant issues starting with algebraic fundamental groups and leading to discussions of several key results in anabelian geometry see Ch.4 of [45]. See also [42] for a survey of several directions in anabelian geometry before 2010, including discussions of some results by Mochizuki which are prerequisites for arithmetic deformation theory.

The fact that the author of this text is not directly working in anabelian geometry can be encouraging for many readers of this text who would typically share this quality.

For any geometrically integral (quasi-compact) scheme X over a perfect field K, the following exact sequence is fundamental

$$1 \to \pi_1^{\mathrm{geom}}(X) \to \pi_1(X) \to \pi_1(\mathrm{Spec}(K)) = G_K \to 1.$$

[16] For every $\varepsilon > 0$ there is a constant c' such that the following inequality holds $N(\mathrm{Disc}_{E_K}) \leqslant c' N(\mathrm{Cond}_{E_K})^{6+\varepsilon} |D_{K/\mathbb{Q}}|^{6+\varepsilon}$ for all elliptic curves E_K over number fields K. This stronger version is equivalent to the Vojta conjecture, as we shall see when we meet it in 2.12, and it shows up in Abstract, the final sentence of §1 and Corollary 4.2 of [33], and on p.17 of [32].

[17] Neither the word "anabelian" nor the Grothendieck letter [13] was mentioned. The author of IUT heard about anabelian geometry for the first time from Takayuki Oda in Kyoto in the summer of 1992.

[18] The four parts of [31] were ready by August 2011 and put on hold for one year. They were posted on the author's webpage in August 2012 and submitted to a mathematical journal.

Here $\pi_1(X)$ is the *algebraic fundamental group* of X, $\pi_1^{\mathrm{geom}}(X) = \pi_1(X \times_K K^{\mathrm{alg}})$, K^{alg} is an algebraic closure of K, see e.g. Prop.5.6.1 of [45]. Suppressed dependence of the fundamental groups on basepoints actually means that objects are often well-defined only up to conjugation by elements of $\pi_1(X)$. Algebraic fundamental groups of schemes over number fields (or fields closely related to number fields, such as local fields or finite fields) are also called *arithmetic fundamental groups*.

If C is a complex irreducible smooth projective curve minus a finite collection of its points, then $\pi_1(C)$ is isomorphic to the profinite completion of the topological fundamental group of the Riemann surface associated to C.

If C is the result of base-changing a curve over a field K to the field of complex numbers, then the analogue for such a curve over K of the displayed sequence (associated to X) discussed in the previous paragraph induces a homomorphism from G_K to the quotient group $\mathrm{Out}(\pi_1^{\mathrm{geom}}(C))$ of the automorphism group of $\pi_1^{\mathrm{geom}}(C)$ by its normal subgroup of inner automorphisms. Belyi proved, using the theorem discussed in 1.1 for elliptic curves, that this map gives an embedding of the absolute Galois group $G_{\mathbb{Q}}$ of $\mathbb{Q}$ into the Out group of the pro-finite completion of a free group with two generators [3]. For readers with background outside number theory I recall that, unlike the case with absolute Galois groups of local fields, we still know relatively little about $G_{\mathbb{Q}}$; hence the Belyi result is of great value.

Recall that a *hyperbolic curve* C over a field K of characteristic zero is a smooth projective geometrically connected curve of genus g minus r points such that the Euler characteristic $2-2g-r$ is negative. Examples include a projective line minus three points or an elliptic curve minus one point. The algebraic fundamental group of a hyperbolic curve is nonabelian.

Anabelian geometry "yoga" for so-called anabelian schemes of finite type over a ground field K (such as a number field, a field finitely generated over its prime subfield, etc.) states that an anabelian scheme X can be recovered from the topological group $\pi_1(X)$ and the surjective homomorphism of topological groups $\pi_1(X) \to G_K$ (up to purely inseparable covers and Frobenius twists in positive characteristic). Thus, the algebraic fundamental groups of anabelian schemes are *rigid*.[19]

In [13], Grothendieck proposed the following questions:

> (a) Are hyperbolic curves over number fields or finitely generated fields anabelian?
> (b) A point x in $X(K)$, i.e. a morphism $\mathrm{Spec}(K) \longrightarrow X$, determines, in a functorial way, a continuous section $G_K \to \pi_1(X)$ (well-defined up to composition with an inner automorphism) of the surjective map $\pi_1(X) \to G_K$. The section conjecture asks if, for a geometrically connected smooth projective curve X over K, of genus > 1, the map from rational points $X(K)$ to the set of conjugacy classes of sections is surjective (injectivity was already known). There is also the question of whether or not the section conjecture could be of use in deriving finiteness results in diophantine geometry.

The Neukirch–Ikeda–Uchida theorem is a birational version of (a) in the lowest dimension. A similar recovery property for fields finitely generated over $\mathbb{Q}$ was proved by Pop. Later Mochizuki proved a similar recovery property for a subfield of a field finitely generated over $\mathbb{Q}_p$. Many more results are known over other types of ground fields, for a survey see e.g. [42].

[19] Compare with the following strong rigidity theorem (Mostow–Prasad–Gromov rigidity theorem) for hyperbolic manifolds: the isometry class of a finite-volume hyperbolic manifold of dimension $\geqslant 3$ is determined by its topological fundamental group, see e.g. [11]. Recall that in étale topology open subschemes of spectra of rings of integers of number fields are, up to 2-torsion, of (l-adic) cohomological dimension 3, see e.g. Th. 3.1 Ch. II of [22].

With respect to (a), important contributions were made by Nakamura and Tamagawa. Then Mochizuki proved that hyperbolic curves over finitely generated fields of characteristic zero are indeed anabelian. Moreover, using nonarchimedean Hodge–Tate theory (also called p-adic Hodge theory), Mochizuki proved that a hyperbolic curve X over a subfield K of a field finitely generated over $\mathbb{Q}_p$ can be recovered functorially from the canonical projection $\pi_1(X) \to G_K$.

The section conjecture in part (b) has not been established. A geometric pro-p-version of the section conjecture fails, see [16] and its introduction for more results. A combinatorial version of the section conjecture is established in [18]. It is unclear to what extent the section conjecture may be useful in diophantine geometry, but [19] proposes a method which may lead to such applications of the section conjecture.

Arithmetic deformation theory, though related to the results in anabelian geometry reviewed above, uses and applies a different set of concepts: mono-anabelian geometry, the nonarchimedean theta-function, categories related to monoid-theoretic structures, deconstruction and reconstruction of ring structures.

2. On arithmetic deformation theory

The task of presenting arithmetic deformation theory on several pages or in several hours is an interesting challenge.[20]

In these notes I attempt to simplify as much as is sensible and to use as little new terminology as is feasible (and to indicate relations with the original terminology of IUT when I use different terminology). As explained in the foreword, I will have to be vague when talking about some of the central concepts and objects of the theory. Some more technical sentences have been moved to the footnotes.

2.1. **Texts related to IUT.**

Inter-universal Teichmüller theory[21] has many prerequisites and offers many innovations.

- *Absolute mono-anabelian geometry*, developed in [30], is an entralling new theory in its own right. It enhances anabelian geometry and brings it to a new level. It plays a pivotal role in IUT.
- The theory of the *nonarchimedean theta-function*, cf. [28] and a review in §1 of [31]-II, is of similar central importance in IUT.
- *Categorical geometry* papers discuss the theory of categories associated to monoid-theoretic structures[22], such as *frobenioids*[23] [27], as well as the theory of anabelioids [24], [26].[24]
- [31]-I-III introduce and study several versions of the theta-link. The key main theorem of the first three parts of IUT is stated in Cor. 3.12 of [31]-III.

[20] In view of the overwhelming novelty of the theory, it is hardly possible to give an efficacious presentation during a standard talk.

[21] The reason for this name is well explained in the Introduction of [31]-I, as well as in the review papers [32] and [33].

[22] The term "monoid-theoretic" in this text corresponds to the term "frobenius-like" in [31]. In IUT, the underlying abstract topological groups associated to étale fundamental groups are often referred to as étale-like structures, see [27]-I, [30]-III. Étale-like structures are functorial, rigid and invariant with respect to the links in IUT, while frobenius-like structures are used to construct the links. The situation which serves as a sort of fundamental model for the terms frobenius-like and étale-like is the invariance of the étale site with respect to the Frobenius morphism in positive characteristic, see Example 3.6 of [31]-IV. Relations between these two types of structures are crucial. Such relations are presented further in these notes without using the terminology of frobenius-like and étale-like.

[23] The theory of frobenioids is motivated by the need to develop a geometry built up solely from Galois theory and monoid-theoretic structures in which a kind of Frobenius morphism on number fields, which does not exist in the usual sense, can be constructed. The availability of such Frobenius morphisms in the theory of frobenioids leads to various analogies between IUT and p-adic Teichmüller theory. For two examples of frobenioids see 2.10.

[24] These papers contain much more material than is necessary for the purposes of IUT. If one understands the philosophy that underlies these papers, it is possible to skip long technical proofs.

- Strengthened versions of notion of a Belyi map obtained in [25] are applied in [29] to prove a new interesting equivalent form of the Vojta conjecture, which is studied in [31]-IV.
- A straightforward computation of the objects that appear in the main theorem of [31]-I-III is summarised in Th. 1.10 of [31]-IV. In Cor. 2.2 of [31]-IV, one makes a choice of a certain prime number l which appears in this computation. This leads to the application to the new form of the Vojta conjecture and hence to the conjectures in 1.3 over any number field.

See 3.2 for a suggestion of possible entries into the theory.

2.2. **Initial data.** There are several equivalent ways to define a normalised degree deg. I will use adeles. Recall that there is a canonical surjective homomorphism from the group $\mathbb{A}_k^\times$ of ideles of a number field k to the group Div_k of complete (i.e. involving archimedean data) divisors associated to k. This group Div_k may be described as the direct sum of value groups associated to the nonarchimedean and archimedean valuations of k. Thus, such a value group is isomorphic to $\mathbb{Z}$ if the valuation is nonarchimedean and to $\mathbb{R}$ if the valuation is archimedean. Similarly, there are canonical surjective homomorphisms from $\mathbb{A}_k^\times$ to the group of complete divisor classes associated to k, to the group of isomorphism classes of complete line bundles on $\mathrm{Spec}(O_k)$ and to the group I_k of fractional ideals of k. For a number field k and an idele $\alpha \in \mathbb{A}_k^\times$ define its (non-normalised) degree $\deg_k$ as $-\log|\alpha|$, where $|\alpha|$ is the canonical module associated to the adelic ring as a locally compact ring by the standard formula $|\alpha| = \mu(\alpha A)/\mu(A)$, and A is any measurable subset of $\mathbb{A}_k$ of non-zero measure with respect to any nontrivial translation invariant measure μ on the underlying additive group of $\mathbb{A}_k$. Then $\deg_k(\alpha) = \deg_{\mathbb{Q}}(N_{k/\mathbb{Q}}\alpha)$, and the degree of the diagonal image of an element of $k^\times$ in $\mathbb{A}_k^\times$ is 0.

Due to the minus sign in the definition of $\deg_k$, it is *minus* the non-normalised degree which can be viewed as the log-volume of αA, where A is, say, the product of the closed balls of radius 1 with centre at 0 for all completions of k, and μ is normalised to give A log-volume 0.

Write $\varinjlim \mathbb{A}_k^\times$ for the inductive limit, with respect to the inclusions induced by field embeddings, of the groups of ideles of all finite extensions k of $\mathbb{Q}$ in a fixed algebraic closure $\mathbb{Q}^{\mathrm{alg}}$. For $\beta \in \varinjlim \mathbb{A}_k^\times$, define its *normalised degree* $\deg(\beta)$ as $|k:\mathbb{Q}|^{-1}\deg_k(\beta)$, where k is any algebraic number field such that β corresponds to an element of $\mathbb{A}_k^\times$. One verifies immediately that this definition does not depend on k. Finally, for an element γ of the perfection of $\varinjlim \mathbb{A}_k^\times$ define its normalised degree $\deg(\gamma)$ as $n^{-1}\deg(\gamma^n)$, where $n \geqslant 1$ is any integer such that $\gamma^n \in \varinjlim \mathbb{A}_k^\times$. Given a fractional ideal in I_k, a complete divisor in Div_k, a complete divisor class, or a line bundle, the normalised degree of any of its lifts to the group of ideles does not depend on the choice of lift (since the local components of such lifts are completely determined up to unit multiples). Denote this degree by the same notation deg.

Let E_F be an elliptic curve over a number field F with split multiplicative reduction. If v is a bad reduction valuation and F_v is the completion of F with respect to v, then the *Tate curve* $F_v^\times/\langle q_v\rangle$, where q_v is the q-parameter of E_F at v and $\langle q_v\rangle$ is the cyclic group generated by q_v, is isomorphic to $E_F(F_v)$, $\langle q_v\rangle \mapsto$ the origin of E_F, see Ch.V of [44] and §5 Ch.II of [43].

Assume further that the 6-torsion points of E_F are rational over F, and F contains a 4th primitive root i of unity.

One works with the hyperbolic curve $X_F = E_F \setminus \{0\}$ over F and the hyperbolic orbicurve $C_F = X_F/\pm 1$ over F obtained by forming the stack-theoretic quotient of X_F by the unique F-involution -1 of X_F.

If k is a field extension of F, then denote $E_k = E_F \times_F k$, $X_k = X_F \times_F k$, $C_k = C_F \times_F k$.[25]

[25] For bad reduction valuations one also works with an infinite $\mathbb{Z}$-(tempered) covering $\mathscr{Y}_v$ of a model $\mathscr{X}_{F_v}$ of X_{F_v} which corresponds to the kernel of the natural surjection from the tempered fundamental group to $\mathbb{Z}$ associated to the universal graph-covering of the dual graph of the special fibre of $\mathscr{X}_{F_v}$. The special fibre of $\mathscr{Y}_v$ is an infinite chain of copies of $\mathbb{P}^1$ joined at 0 and ∞.

Define an idele $q_{E_F} \in \mathbb{A}_F$: its components at archimedean and good reduction valuations are taken to be 1; its components at bad valuations are taken to be q_v, where q_v is the q-parameter of the Tate elliptic curve $E_F(F_v) = F_v^\times / \langle q_v \rangle$. The number n_v of components of E_F at a bad reduction valuation v is exactly the value of the surjective discrete valuation $v\colon F_v^\times \to \mathbb{Z}$ at q_v. Thus, $\deg_F(q_{E_F})$ is the LHS of the inequality of the Szpiro conjecture in 1.3. *The ultimate goal of the theory is to give a suitable bound from above on* $\deg(q_{E_F})$.

2.3. **A brief outline of the proof and a list of some of the main concepts.** Conventional scheme-theoretic geometry is insufficient for the purposes of arithmetic deformation theory. This is one of the reasons why it was not developed earlier. IUT goes beyond standard arithmetic geometry. Still, it remains quite geometric and categorical. In its application to the conjectures of 1.3 it does not need to use more from analytic number theory than the prime number theorem.

Fix a prime integer $l > 3$ which is relatively prime to the bad reduction valuations of E_F, as well as to the value n_v of the local surjective discrete valuation of the q-parameter q_v for each bad reduction valuation v.

In 2.12, l will be chosen to be relatively large, so in IUT one often views $\mathbb{Z}/l\mathbb{Z}$ as a kind of approximation to $\mathbb{Z}$, see §1.3 of [23] for more on this.[26]

Assume that the extension K of F generated by the l-torsion points of E_F has Galois group over F isomorphic to a subgroup of $GL_2(\mathbb{Z}/l\mathbb{Z})$ which contains $SL_2(\mathbb{Z}/l\mathbb{Z})$.[27]

Due to various reasons motivated by Hodge–Arakelov theory, cf. §1 of [32], §1 of [33], it makes a lot of sense to look at the *monoid-theoretic maps* defined, for bad reduction valuations v, on the submonoid of the multiplicative group $F_v^\times$ generated by units and q_v as follows:

$$q_v \longmapsto q_v^{m^2}, \qquad u \longmapsto u \quad \text{for all } u \in O_{F_v}^\times,$$

where O_{F_v} is the ring of integers of F_v, m is a fixed integer such that $1 \leqslant m \leqslant (l-1)/2$.

The element $q_v^{m^2}$ will be viewed as a *special value* of a certain nonarchimedean theta-function.

Choose a $2l$th root $\underline{\underline{q}}$ of q. We are now led to the study of a monoid-theoretic map which forms part of a so-called *theta-link*, and which at bad reduction valuations can be viewed as the assignment

$$\underline{\underline{q}} \longmapsto \left\{\underline{\underline{\Theta}}\left(\sqrt{-q^m}\right) = \underline{\underline{q}}^{m^2}\right\}_{1 \leqslant m \leqslant (l-1)/2}.$$

This map is not scheme-theoretic. Its application may be viewed as a deconstruction of the ring structure.[28] To reconstruct the ring structure, one uses *generalised Kummer theory* (cf. 2.6), *two types of symmetry* (cf. 2.7), *rigidities* (cf. 2.9) and *splittings* (cf. 2.7), all of which are closely related to the theta-link (cf. 2.7).

In order to reconstruct portions of the ring structure related to the theta-link, it is necessary to make use of (archimedean and nonarchimedean) logarithms, in the form of a so-called *log-link*, cf. 2.8. The theory of the log-link also involves the mono-anabelian geometry, cf. 2.4, developed in [30]-III. Moreover, one must make use of infinitely many log-links.

Various copies of the theta-link will form horizontal arrows between two vertical lines formed by the log-links of a *log-theta-lattice*.

---

[26] When the prime number l is chosen in Cor. 2.2 of [31]-IV, some of these conditions on l may be slightly weakened, by treating certain bad reduction valuations of E_F as if they are good reduction valuations.

[27] One also assumes that C_K is a terminal object in the category whose objects are generically scheme-like algebraic stacks Z that admit a finite étale morphism to C_K, and whose morphisms are finite étale morphisms of stacks $Z_1 \longrightarrow Z_2$ defined over K (that do not necessarily lie over C_K), this assumption implies that C_F has a unique model over the field F_{mod} defined in 2.6, c.f. Rk 3.1.7(i) of [31]-I.

[28] This map will be discussed further in 2.7.

The main theorem of IUT is a bound on log-volumes of the form

$$-\deg(q_E) \leqslant -\deg(\Theta_E),$$

which is subject to the condition that the term on the RHS, which by definition is the log-volume of the union of possible images of theta-data after applying the theta-link, subject to certain indeterminacies, is not equal to $+\infty$. This bound has a lot of meaning from the point of view of IUT: it is a *bound on deformation size* of theta-data with respect to the *indeterminacies associated to the theta- and log-links*. Such a bound is obtained in the final portion of the first three parts of [31] as the main theorem of IUT in [31]-III. Note the minus sign on the LHS of this bound in comparison to the goal stated at the end of the previous subsection.

A further relatively straightforward computation in [31]-IV of the RHS of this inequality, which follows essentially from its definition in [31]-III, will show that

$$-\deg(\Theta_E) \leqslant a(l) - b(l)\deg(q_E)$$

with real numbers $a(l), b(l) > 1$ depending on $l > 3$. Hence, combining this with the previous bound, one obtains a bound $\deg(q_E) \leqslant a(l)(b(l)-1)^{-1}$, see 2.12.

Then a suitable choice of the prime number l will lead to a bound on $\deg(q_E)$ of the right form which, after a bit more work, implies the diophantine inequalities (a)–(e) of 1.3.

The notation $-\deg(\ )$ in this text corresponds to the notation $-|\log(\ )|$ in [31]-III-IV.

Thus, the following list of some of the main concepts and methods of IUT which will be discussed in the following subsections comes very naturally. For a continuation of the list see 2.13.

- ◇ Mono-anabelian geometry uses hyperbolic curves, which in IUT will always be related to a fixed, given elliptic curve, to recover the ring structure of number fields and their completions, [30]-III. Mono-anabelian geometry plays an important role in the construction of multiradial algorithms in [31]-II-III.
- ◇ One chooses a prime number l and works with the ring $\mathbb{Z}/l\mathbb{Z}$, which can also be viewed as an approximation to the ring $\mathbb{Z}$, and with the l-torsion points of the elliptic curve. There are two types of symmetry associated to the choice of l, which play a key role in IUT, cf. [31]-I-III.
- ◇ The nonarchimedean theta-function and its values at torsion points, generalised Kummer (and log-Kummer) theory and the two types of symmetry are used in the construction of the central object of IUT, the theta-link, and closely related to associated rigidities and synchronisations, cf. [28], [31]-I-III.
- ◇ One has to involve the nonarchimedean logarithm map as well, in the form of the log-link, cf. [31]-III.
- ◇ Application of the theta-link and log-link deconstructs the ring structures, in the sense that it treats the underlying additive and multiplicative structures of the rings involved as separate monoid-theoretic structures. The ring structures are reconstructed via a series of algorithms by using deep results from anabelian geometry and generalised Kummer theory and working with the log-theta-lattice, cf. [30]-III and [31]-I-III.
- ◇ Bounding the size of the deformation arising from the theta-link by taking into account three associated indeterminacies, and then making a further (easier) computation of the RHS of the bound, which is ultimately applied for a suitable choice of the prime number l, leads to a bound of the type needed for the conjectured inequalities in diophantine geometry.

2.4. **Mono-anabelian geometry and multiradiality.** A more powerful version of anabelian geometry is developed in [30]. It is called *absolute mono-anabelian geometry*. The classical approach to anabelian geometry centers around a comparison between two geometric anabelian objects via their algebraic fundamental groups. Mono-anabelian geometry centers around the task of establishing *topological group-theoretic algorithms* which

require only the following input datum: a *topological group* which just happens to be isomorphic to the algebraic fundamental group of a scheme (satisfying certain conditions). Mono-anabelian geometry algorithmically recovers the ring structure of an object or a priori scheme-theoretic construction, operation, property from the topological group structure of a group of symmetries such as the Galois group or algebraic fundamental group.

For example, compare the statement of the Neukirch–Ikeda–Uchida theorem in 1.1 with the theorem proved by Mochizuki, cf. Th. 1.9 of [30]-III,

> The number field F can be reconstructed via an algorithmic procedure from the arithmetic fundamental group $\pi_1(X_F)$ (which surjects onto the absolute Galois group G_F).

Unlike the case with the Neukirch–Ikeda–Uchida theorem, the mono-anabelian algorithms of Th. 1.9 of [30]-III are functorial with respect to change of the base field and compatible with localisation.[29] These properties are crucial for applications in IUT.

Working with hyperbolic curves over number fields adds a geometric dimension. Certain aspects of IUT relate the two ring-theoretic dimensions of the function field of such a hyperbolic curve (one of which is arithmetic, the other geometric) to the two combinatorial dimensions (constituted by the additive and multiplicative structures) of a ring.[30]

In IUT, one works with hyperbolic (orbi)curves such as X_k, C_k, as well as related objects, see 2.2, over number fields k and their completions. The arithmetic fundamental groups of such geometric objects are used to reconstruct the ring structure of the base field, by applying the theory of [30]-III. [31]

When working with fundamental groups, the issue of basepoints has to be carefully addressed. The existence of different basepoints in the domain and range of the theta-link and log-link implies that one must consider two *different universes* associated to two distinct ring theories which in general cannot be related by means of a ring homomorphism, cf. §I3 of [31]-I. This inter-universal aspect gives rise to the name of IUT. The main type of mathematical object which makes sense simultaneously in both the universes is a topological group.

IUT applies mono-anabelian reconstruction algorithms to arithmetic fundamental groups that appear in one universe in order to obtain descriptions of objects constructed from such arithmetic fundamental groups that make sense in another universe. [31] uses the terminology of a wheel and spokes.

One can think of reconstruction algorithms as functorial algorithms from a radial category to the centre (core) category, say, as a wheel with a centre (core) and spokes, that satisfies the property that descriptions of objects which arise on one spoke make sense from the point of view of another spoke. The principal example of this sort of situation arises by considering the data in the domain and codomain of the theta-link. Using the same analogy, an algorithm is called *multiradial* if it expresses objects constructed from a given spoke in terms of objects that make sense from the point of view of other spokes. Multiradial algorithms are compatible with simultaneous execution at multiple spokes, which is important for IUT.

To obtain multiradial algorithms, it is sometimes necessary to allow for some sort of *indeterminacy* in the descriptions that appear in the algorithms of the objects constructed from the given spoke. See 2.9 for three

[29] for more on mono-anabelian reconstruction for number fields see a recent preprint [17]

[30] see Rk 2.3.3 (ii) of [31]-III for more details

[31] In this context, observe that for local fields, unlike number fields, there is a description of the associated absolute Galois group (in odd residue characteristic) given by the Yakovlev–Jannsen–Wingberg theorem, see e.g. §5 Ch.VII of [40]. However, unlike the number field case, to recover an isomorphism of local fields from an isomorphism of topological groups between the respective absolute Galois groups without using hyperbolic curves, one needs to know in addition that this isomorphism is compatible with the respective upper ramification group filtrations. This is a theorem proved independently by Mochizuki and Abrashkin, see e.g. 8.3 of Ch.IV of [10] and the references therein. The proof by Mochizuki is very short and uses p-adic Hodge theory. For more details see §3 of [30]-I.

indeterminacies which play a key role in the computation of volume deformation, and whose effects result in the ε term in the conjectures of 1.3.

For more examples of multiradiality see §2 of [33] and the Introduction and Examples 1.8-1.9 of [31]-II.

2.5. **Nonarchimedean theta-functions.** Let L be a local field of characteristic zero with finite residue field. Denote by $\mathbb{C}_L$ the completion of an algebraic closure of L. A holomorphic function on $\mathbb{C}_L^\times$ defined over L is a function $\mathbb{C}_L^\times \to \mathbb{C}_L$ which is represented by an everywhere convergent element of $L((X))$. A meromorphic function on $\mathbb{C}_L^\times$ defined over L is an element of the field of fractions of the ring of holomorphic functions on $\mathbb{C}_L^\times$ defined over L.

Let $q \in L$ be a non-zero element of the maximal ideal of the ring of integers of L (this q will eventually be taken to be the q-parameter q_v of the Tate curve $E_F(F_v) \simeq F_v^\times/\langle q_v\rangle$, where $L = F_v$, for bad reduction primes v of E, see Ch.5 of [44]). An elliptic function with period q on L is a meromorphic function on $\mathbb{C}_L^\times$ defined over L and invariant with respect to the map $u \mapsto qu$, so it yields a function on $\mathbb{C}_L^\times/\langle q\rangle$. A theta-function on $\mathbb{C}_L^\times$ defined over L, of type au^m, $a \in \mathbb{C}_L^\times$, $m \in \mathbb{Z}$, is a holomorphic function on $\mathbb{C}_L^\times$ defined over L which satisfies a functional equation $f(u) = au^m f(qu)$. Every elliptic function can be written as the quotient of two theta-functions of the same type, see pp.14-15 of [46].

The following choice of *nonarchimedean theta-function* of type $-u$ is convenient, p.15 of [46], in view of the location of its zeros and poles

$$\theta(u) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n(n-1)/2} u^n = (1-u)\prod_{n\geqslant 1}\big((1-q^n)(1-q^n u)(1-q^n u^{-1})\big), \qquad u \in \mathbb{C}_L^\times,$$

where the last equality follows from the Jacobi triple product formula.

It is easy to see that if $a_v \in L^\times$, $m_v \in \mathbb{Z}$ and $\sum_{v=1}^n m_v = 0$, then the function $\prod_{v=1}^n \theta(a_v u)^{m_v}$ is of type $\prod_{v=1}^n a_v^{m_v} \in L^\times$. This property, which is used in Tate's formula for the local height pairing (cf. p. 338 of [2]), yields an interesting relationship between the multiplicative properties of the nonarchimedean theta-function and the underlying multiplicative structure of a local field. In this sense, it is reminiscent of the theta-link, which plays a central role in IUT.

Just as in the classical complex theory, elliptic functions on L with period q can be expressed in terms of θ, a property which highlights the central role of nonarchimedean theta-functions in the theory of functions on the Tate curve. For more information see §2 Ch.I and §5 Ch.II of [43] and p. 306-307 of [38].

The nonarchimedean theta-function is of course related to the complex theta-function

$$\theta(z,\tau) = \sum_{n\in\mathbb{Z}} \exp(\pi i n^2\tau + 2\pi i n z), \qquad z,\tau \in \mathbb{C}, \quad \Im m(\tau) > 0,$$

which is equal to $\sum_{n\in\mathbb{Z}} q^{n^2/2}u^n = \theta(-q^{1/2}u)$, $u \in \mathbb{C}$, via the change of variables $q = \exp(2\pi i\tau), u = \exp(2\pi i z)$.

The theta-function

$$\ddot{\Theta}(u) = -u^{-1}\theta(u^2) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n(n+1)/2} u^{2n+1}$$

in Prop. 1.4 of [28] where u equals $\dot{U}$ defined there and q equals q_X defined there, is of type q^2u^4. Moreover $\ddot{\Theta}(q^{1/2}u) = -q^{-1/2}u^{-2}\ddot{\Theta}(u)$. The function $\ddot{\Theta}(u)$ extends to a meromorphic function[32] and satisfies the following unusual property among meromorphic functions: its divisor of poles is contained in the special fibre, while its divisor of zeroes does not contain any irreducible component of the special fibre.

[32] on a certain finite covering $\ddot{\mathscr{Y}}_v$ of the covering $\mathscr{Y}_v$ discussed in footnote 25

We still assume that $l>3$ as in 2.3 and F contains i as in 2.2. Example 3.2 (ii) of [31]-I introduces a function

$$\underline{\underline{\Theta}}(u)=\underline{\underline{\Theta}}_{\underline{v}}(u)=\left(\ddot{\Theta}(i)/\ddot{\Theta}(u)\right)^{1/l},$$

which is well-defined up to multiplication by roots of unity of order dividing $2l$ (with q equal to $q_{\underline{v}}$ defined there).

One further assumes that the residue characteristic of the local field L is odd. The functional equation for θ implies that

$$q^{m^2/2}\,\ddot{\Theta}\left(i\,\sqrt{q^m}\right)=\ddot{\Theta}(i).$$

Choose a $2l$th root $\underline{\underline{q}}$ of q. Then

$$\underline{\underline{q}}^{m^2}=\underline{\underline{\Theta}}\left(\sqrt{-q^m}\right)$$

up to multiplication by roots of unity of order dividing $2l$.

These special values of the theta-function for $1\leqslant m\leqslant (l-1)/2$, i.e. the values at points separated by periods $q^{m/2}$ from the point $\pm i$, are very distinguished from several points of view.[33] They are of central importance for IUT.

2.6. **Generalised Kummer theory.** For an open subgroup H of a Galois or arithmetic fundamental group acting on an abelian group M, Kummer theory deals with the natural homomorphism

$$M^H\longrightarrow H^1(H,\mathrm{Hom}(\mathbb{Q}/\mathbb{Z},M))$$

obtained by considering the divisibility of elements of the abelian group M. Injectivity of the Kummer map, when available, is very useful.

Kummer theory (more precisely, truncated Kummer theory) of the line bundles associated to nonarchimedean theta-functions is developed in [28]. Note that the naive theory of theta functions is not sufficient for the purposes of IUT, for more details and interesting discussions of aspects of the étale theta function see recently added Rk 2.3.4 of [31]-III.

Kummer theory provides a bridge between monoid-theoretic structures and arithmetic fundamental group structures associated to the theta-function and theta-values (see [28], Fig. I.1 of [31]-II), as well as to a number field and its completions (see Example 5.1 of [31]-I, where the mono-anabelian geometry of [30]-III is applied to reconstruct a number field and its completions from the arithmetic fundamental groups of hyperbolic orbicurves that arise as finite étale coverings of C_F).[34] One important aspect of the Kummer theory applied in IUT is the issue of *cyclotomic rigidity*, i.e. of establishing algorithms for reconstructing natural isomorphisms between cyclotomes that arise from the geometric fundamental group and cyclotomes that arise from monoid-theoretic data (see Def. 1.1 (ii) of [31]-II in the theta-function case, Example 5.1 of [31]-I in the number field case).

Denote by F_{mod} the field of moduli of the curve E_F. Assume that F is Galois over F_{mod}. Choose subsets V_F, V_K of valuations of F, K such that the inclusion of fields $F_{\mathrm{mod}}\subset F\subset K$ induces a bijection between V_K, V_F, and the set V_{mod} of all valuations of F_{mod}.[35] For a valuation v of F_{mod} denote by K_v the completion of K with respect to the element of V_K corresponding to v.

This data determines, up to K-isomorphism, a finite étale covering $\underline{C}_K\longrightarrow C_K$ of degree l which satisfies the following property: the natural covering $E_K\longrightarrow E_K$ determined by multiplication by l factors as a composite

[33] see Rk 2.5.1 of [31]-II and Rk 2.2.2 of [31]-III for more on this

[34] Using the terminology of IUT, Kummer theory relates certain étale-like structures with certain frobenius-like structures, see also footnote 22.

[35] It is assumed that the set of bad reduction valuations in V_K of odd residue degree is nonempty. There are further technical conditions that must be imposed on V_K; these conditions are discussed in detail in Def. 3.1 of [31]-I (where V_K corresponds to $\underline{\mathbb{V}}$).

$E_K \longrightarrow \underline{E}_K \longrightarrow E_K$, where the covering $\underline{E}_K \longrightarrow E_K$ is the covering determined by the base-changed covering $\underline{X}_K := \underline{C}_K \times_{C_F} X_F \longrightarrow X_K$ and corresponds to a quotient isomorphic to $\mathbb{Z}/l\mathbb{Z}$ of the l-torsion submodule of $E_K(K)$ that restricts at bad reduction valuations of V_K of odd residue degree to the quotient arising from coverings of the dual graph of the special fibre. In addition, at bad reduction valuations $v \in V_K$ of odd residue degree one considers a natural finite étale covering $\underline{\underline{X}}_v \longrightarrow \underline{X}_K \times_K K_v$ of degree l by extracting lth roots of the theta-function. These coverings play an important role in the generalised Kummer theory employed in IUT.

2.7. **The theta-link and two types of symmetry.** The setting up of several versions of the theta-link is technical, and a large part of the three papers [31]-I-III is dedicated to it, see also the foreword.[36] In the following, I discuss aspects of IUT that are related to various versions of the theta-link.

At bad reduction valuations of E_F of odd residue characteristic, a simplified version of the theta-link, cf. [31]-I, uses the theta-function and revolves around a certain morphism of local monoid-theoretic structures

$$\underline{\underline{q}} \longmapsto \underline{\underline{\Theta}},$$

while the main version of the theta-link dealt with in this text, cf. [31]-II-III, uses the theta-values and revolves around a certain morphism of local monoid-theoretic structures

$$\underline{\underline{q}} \longmapsto \left\{\underline{\underline{\Theta}}\left(\sqrt{-q^m}\right) = \underline{\underline{q}}^{m^2}\right\}_{1 \leqslant m \leqslant (l-1)/2},$$

with the identity map on units (in an algebraic closure of F_v) or units modulo roots of unity, acted upon by the absolute Galois group of F_v. One then extends these local theta-links to other valuations (actually valuations in the set V_K, see 2.6), in such a way as to satisfy the product formula.

For bad reduction valuations of odd residue characteristic, the latter version of the theta-link amounts to an *arithmetic deformation* of the local structure of the local field associated to the valuation, sending units of the ring of integers via the identity map to the units and sending $\underline{\underline{q}}^n$ to $\underline{\underline{q}}^{m^2 n}$, $n \geqslant 1$, where the integer m runs between 1 and $(l-1)/2$. This monoid-theoretic morphism is not compatible with the ring structure, i.e. *the theta-link is not scheme-theoretic*.

The monoid-theoretic structures that appear in this theta-link consist of two local structures

- units modulo torsion $O_L^\times/\mathrm{Tor}(O_L^\times)$ and
- theta-values such as $\underline{\underline{\Theta}}\left(\sqrt{-q^m}\right) = \underline{\underline{q}}^{m^2}$, which are well-defined up to multiplication by roots of order dividing $2l$,

and one global structure, namely,

- the global realified frobenioid[37] associated to the number field in the product of all the local data.

Monoid-theoretic structures are of essential importance in IUT, since they allow one to construct various gluing isomorphisms. The use of Galois and arithmetic fundamental groups gives rise to canonical splittings of objects arising from such gluing isomorphisms by applying various tautological Galois-equivariance properties of such gluing isomorphisms.

The computation of the theta-link can be viewed as a sort of passage from monoid-theoretic data to such canonical splittings involving arithmetic fundamental groups, by applying generalised Kummer theory, together with various multiradial algorithms which make essential use of mono-anabelian geometry.

[36] Each theta-link consists of the collection of all isomorphisms between certain data associated to the respective theatres of type 1 in the domain and codomain of the theta-link, see footnote 38. The main distinctive feature of each of the two types of theta-link discussed in this subsection is represented by the monoid-theoretic map in the corresponding display.

[37] see footnote 23

Two types of symmetry are closely related to the setting up of the theta-link and, very importantly, of a central object in IUT not discussed in these notes, namely, a (*theta-number field-Hodge-*) *theatre*.[38] They are denoted $\mathbb{F}_l^{\triangleright\!\!\triangleleft\pm} = \mathbb{F}_l \rtimes \{\pm 1\}$ and $\mathbb{F}_l^{*} = \mathbb{F}_l^{\times}/\{\pm 1\}$ where $\mathbb{F}_l \simeq \mathbb{Z}/l\mathbb{Z}$ arises from the l-torsion points of E, cf. [31]-I-III. Elements of of $\mathbb{F}_l$ (in the case of $\mathbb{F}_l^{\triangleright\!\!\triangleleft\pm}$) or $\mathbb{F}_l^{*}$ (in the case of $\mathbb{F}_l^{*}$) are called labels.

The $\mathbb{F}_l^{\triangleright\!\!\triangleleft\pm}$*-symmetry* arises from the action of π_1^{geom} and is closely related to the Kummer theory surrounding the theta-values. There is a natural isomorphism $\mathrm{Aut}_K(\underline{X}_K) \xrightarrow{\sim} \mathbb{F}_l^{\triangleright\!\!\triangleleft\pm}$, cf. Def. 6.1(v) of [31]-I.

This symmetry is

- of an essentially geometric nature, i.e. corresponds to the geometric portion of the arithmetic fundamental groups involved
- additive $z \mapsto \pm z + a$, $a \in \mathbb{F}_l$
- compatible with and applied to establish *conjugate synchronisation* (i.e. permuting copies of local absolute Galois groups associated to distinct labels without inducing conjugacy indeterminacies)
- compatible with the nonarchimedean logarithm and the (closely related) construction of the log-shell
- of a somewhat non-multiradial nature[39].

The $\mathbb{F}_l^{*}$*-symmetry* arises from the action of the absolute Galois group of certain number fields and is closely related to the Kummer theory surrounding these number fields. The group $\mathbb{F}_l^{*}$ is isomorphic to a subquotient of $\mathrm{Aut}(\underline{C}_K)$ induced via the natural inclusion $\mathrm{Aut}(\underline{C}_K) \hookrightarrow \mathrm{Aut}(K)$ (cf. Rk 2.6.1 of [28]) by a subquotient of $\mathrm{Gal}(K/F)$, see also Example 4.3 of [31]-I.

This symmetry is

- of an essentially arithmetic nature, i.e. it corresponds to the global arithmetic portion of the arithmetic fundamental groups involved
- multiplicative (by definition)
- used in label bookkeeping to separate the label 0 from the nonzero labels
- closely related to the operation of for descending from K to the field of definition F_{mod} of E_F (cf. Rk 6.12.6 (iii), (iv) of [31]-I).
- of an essentially multiradial nature.

Each type of symmetry includes a global portion.[40]

The various labels associated to the two types of symmetry are glued together in the following way: $\pm a \in \{-(l-1)/2, \ldots, -1, 0, 1, \ldots, (l-1)/2\}$ is identified with $a \in \{1, \ldots, (l-1)/2\}$.[41]

The issue of basepoints of fundamental groups is closely related to the importance of synchronising conjugacy indeterminacies of local Galois groups. Conjugate synchronisation is a specific system of isomorphisms,

[38] There is a theatre of type 1, denoted $\mathscr{HT}^{\Theta^{\pm\mathrm{ell}}\mathrm{NF}}$ in [31]-I, which is a certain system of categories obtained by gluing together various types of frobenioids (cf. [27] and see also footnote 23 and 2.10), taking into account theta-data and number field-data. To every theatre of type 1 one associates a theatre of type 2, denoted $\mathscr{HT}^{\mathscr{D}\text{-}\Theta^{\pm\mathrm{ell}}\mathrm{NF}}$ in [31]-I, which is a certain system of categories obtained by gluing together various types of of base categories. Many of these base categories are isomorphic to full subcategories of finite étale covers of appropriate hyperbolic curves. Each theatre consists of two portions, corresponding to the two types of symmetry discussed in this subsection; these two portions are glued together in a fashion that is compatible with the gluing of labels discussed in this subsection. For complete definitions see §3-§6 of [31]-I. Each lattice point of the log-theta-lattice discussed in the following subsection denotes a theatre of type 1.

[39] This additive symmetry is, unlike the multiplicative symmetry, non-multiradial at an a priori level. On the other hand, ultimately it is nevertheless used in various multiradial algorithms, cf. the discussion of Rk 3.11.2 (ii) in [31]-III.

[40] The global $\mathbb{F}_l^{\triangleright\!\!\triangleleft\pm}$-symmetry of $\underline{X}_K$ only extends to a ± 1-symmetry of the local coverings $\underline{\underline{X}}_v$, while the global $\mathbb{F}_l^{*}$-symmetry of $\underline{C}_K$ only extends to the identity-symmetry of the local coverings $\underline{\underline{X}}_v$ defined in 2.6.

[41] for more on this see Rk 3.11.2 (ii) of [31]-III

free from conjugacy indeterminacies, between local absolute Galois groups (as topological groups) at the l-torsion points of the elliptic curve where the values of the nonarchimedean theta-function are computed.

Once one has established conjugate synchronisation, Kummer theory is applied to a collection of several special values of the theta-function, by considering the action of a single Galois group that acts simultaneously on the Nth roots of all of them in a fashion compatible with the Kummer theory of the ground field.

In IUT it is necessary to isolate the two types of symmetry from each other in order to establish conjugate synchronisation using the $\mathbb{F}_l^{\times\pm}$-symmetry (note that conjugation by elements of absolute Galois groups of number fields is incompatible with this objective), and in order to work with global base fields from an anabelian point of view using the $\mathbb{F}_l^*$-symmetry.

Conjugate synchronisation yields isomorphisms of monoids associated to different labels in $\mathbb{F}_l$, diagonal submonoids inside the product of the monoids associated to the various labels in $\mathbb{F}_l$ and in $\mathbb{F}_l^*$ and an isomorphism between the monoid associated to the label $0 \in \mathbb{F}_l$ and the diagonal submonoid in the latter product.

2.8. **Nonarchimedean logarithm, log-link, log-theta-lattice, log-shell.** The nonarchimedean logarithm map

$$\log\colon O_L^\times \longrightarrow L$$

is defined on units of the ring of integers of a local field L as the map which sends $1-\alpha \mapsto -\sum_{n\geqslant 1}\alpha^n/n$ for α in the maximal ideal of O_L, and which sends multiplicative representatives of the finite residue field in O_L to 0. The logarithm is compatible with arbitrary automorphisms, such as Galois automorphisms, of the topological field L.

The theta-link requires the use of logarithms, since the logarithm transforms multiplication into addition (and thus allows one to reconstruct certain additive structures from certain multiplicative structures). In other words, there is no natural action of the theta-values on the multiplicative monoid of units modulo torsion, but there is a natural action of the theta-values on the logarithmic image of this multiplicative monoid.

The multiplicative structures on either side of the theta-link are related by means of the value group portions; the additive structures on either side of the theta-link are related by means of the unit group portions, shifted once via the log-link, in order to transform the multiplicative structure of these unit group portions into an additive structure.

Locally the log-link can be thought of as associating to the multiplicative monoid $O\setminus\{0\}$ of non-zero elements of the ring of integers O of $\mathbb{C}_L$ (see 2.5) acted upon by an arithmetic fundamental group the copy of this multiplicative monoid that arises from the copy of the ring O whose underlying additive module is a submodule of $\log(O^\times)\otimes\mathbb{Q}$.

Thus, one obtains a two-dimensional lattice, which is referred to as the *log-theta-lattice*, each of whose upward-pointing vertical arrows corresponds to an application of the log-link, and each of whose rightward-pointing horizontal arrows $(n,m)\to(n+1,m)$ corresponds to an application of a certain theta-link whose construction depends, in an essential way, on the log-link $(n,m-1)\to(n,m)$. The main results of IUT require the use of just two infinite neighbouring vertical lines of arrows of the lattice, i.e. corresponding to the lattice points (n,m), where n equals 0 or 1, together with the horizontal arrow between the lattice points $(0,0)$ and $(1,0)$.

One of the main aims of [31] is the study of mathematical structures associated with the log-theta-lattice.

The theta-link involves two distinct ring/scheme theories, two theatres (see footnote 38) in the domain and codomain of the theta-link, with their multiplicative structures related via nonarchimedean theta values (monoids that appear in the domain of the theta-link and in its codomain are subject to quite different Kummer theories). The task to understand how much their additive structures differ from each other is accomplished

via the use of Kummer correspondence and mono-anabelian reconstruction algorithms. It is a highly interesting question if the concept of the theta-link and its realisation may have more applications, with appropriate modifications, elsewhere in arithmetic geometry.

The log-link does not commute with the theta-link. This non-commutativity difficulty is resolved in IUT via the use of log-shells and applications of the log-Kummer correspondence. *A log-shell* is a very useful common structure for the log-links in one vertical line. Its nonarchimedean part is a slightly adjusted form of the image of the local units via the nonarchimedean logarithm. Namely, by definition it is the compact subgroup

$$(p^*)^{-1}\log(O_L^\times)$$

where $p^*=p$ if p is odd and $2^*=4$, see [30]-III, [31]-III for more details. The log-shell associated to a complex archimedean field is the closed ball of radius π.

Relevant Kummer isomorphisms are not compatible with the log-link at the level of elements; however, the log-shell contains the images of the Kummer isomorphisms associated to both the domain and the codomain of the log-link, cf. [30]-III, [31]-III.

2.9. **Rigidities and indeterminacies.** [28] establishes several rigidity properties of the theta-function, which can be interpreted as multiradiality properties in the context of IUT. The following rigidities, which may be formulated in terms of suitable algorithms, are very useful in IUT:

- (discrete rigidity) one can work with $\mathbb{Z}$-powers instead of $\widehat{\mathbb{Z}}$-powers of q;
- (constant multiple rigidity) the monoid generated by $O_L^\times$ and non-negative powers of $\underline{\underline{\Theta}}$ has a canonical splitting (up to multiplication by $2l$th roots of unity) via evaluation at a 2-torsion point;
- (cyclotomic rigidity) an isomorphism between two copies of $\widehat{\mathbb{Z}}$ endowed with Galois actions, one of which arises from the roots of unity of the base field, the other of which is a certain subquotient of a fundamental group.

Note that in IUT, the copies of $\hat{\mathbb{Z}}$ (or quotients of $\hat{\mathbb{Z}}$) which appear in discussions of cyclotomic rigidity are referred to as cyclotomes. For more see the Introduction of [31]-II and Rks 2.1.1, 2.3.3 of [31]-III.

When relating monoid-theoretic structures with Galois structures via generalised Kummer maps and the use of the theta-function, one must contend with three associated indeterminacies which can be viewed as effects of arithmetic deformation:

- (Ind1) is closely related to the action of $\mathrm{Aut}(G_L)$ and arises from the requirement of compatibility with the permutation symmetries of the Galois and arithmetic fundamental groups associated with vertical lines of the log-theta-lattice;
- (Ind2) is closely related to the action of a certain compact group[42], which includes $\widehat{\mathbb{Z}}^\times$, on $\log(O_L^\times)$ and arises from the requirement of compatibility with the horizontal theta-link;
- (Ind3) arises from a certain (upper semi-)compatibility of the Kummer isomorphism with the log-links associated to a single vertical line of the log-theta-lattice.[43]

2.10. **The role of global data.** Global data is used

- for synchronizing $\pm$-indeterminacies associated to special fibres[44]

[42] the group of G_L-isometries of the units of the ring of integers of an algebraic closure of L modulo roots of unity

[43] This compatibility may be thought of as a weakened version of the usual notion of commutativity of a diagram of morphisms: instead of considering compatibility at the level of individual elements of objects of the diagram, one considers compatibility of inclusions of certain subsets of these objects.

[44] see Rk 6.12.4 (iii) of [31]-I

- in the product formula for monoids
- to conclude that global elements integral everywhere are roots of unity, hence belong to the kernel of log
- when one applies the prime number theorem in [31]-IV
- when one reconstructs, via mono-anabelian algorithms applied to the arithmetic fundamental groups of hyperbolic curves over number fields, the global and local ring structures and the ring homomorphism from the ring of global elements to the adelic ring.

Compare the first item with the Bogomolov proof[45] of the Szpiro inequality over $\mathbb{C}$ discussed in 1.3.[46]

It is a good time to give two examples of categories related to structures used in IUT. These two examples may be thought of as isomorphic monoid-theoretic structures (which, nevertheless, are defined slightly differently) arising from the number field F_{mod} (together with the set of valuations V_K discussed above) that are associated to the collection of complete arithmetic line bundles or, alternatively, to the adeles, equipped with the action of the non-zero global elements. These categories are defined as follows (see Example 3.6 of [31]-III for more details):

(i) *rational function torsion version*: an object of this category is an $F_{\mathrm{mod}}^{\times}$-torsor T equipped with a collection of trivialisations t_v, for each $v \in V_K$, of the torsor T_v associated to T by changing the structure group via the natural map $F_{\mathrm{mod}}^{\times} \longrightarrow K_v^{\times}/O_{K_v}^{\times}$ determined by v; an elementary morphism between $\{T, t_v\}$ and $\{T', t_v'\}$ is an isomorphism $T \longrightarrow T'$ of $F_{\mathrm{mod}}^{\times}$-torsors which maps the trivialisation t_v to an element of the $O_{K_v} \setminus \{0\}$-orbit of t_v'; a morphism is given by an integer $n > 0$ and an elementary morphism from the nth tensor power of the first object to the second object;

(ii) *local fractional ideal version*: an object of this category is a collection of closed balls centred at 0 in the completions of K at the valuations of V_K such that all but finitely many of these closed balls coincide with the respective local rings of integers; an elementary morphism between two such objects is given by multiplication by an element of $F_{\mathrm{mod}}^{\times}$ which maps the local closed balls of the first object into the local closed balls of the second object; a morphism is an integer $n > 0$ and an elementary morphism from the nth tensor power of the first object to the second object.

These two categories are examples of frobenioids [27], see also footnotes 23 and 38. They are quite different from each other from the point of view of multiradiality issues. It is the second category which is subject to distortion when Kummer theory is applied in the context of the log-links. This distortion is closely related to the upper semi-compatibility mentioned in (Ind3) above, as well as to the fact that the second category, unlike the first, is well suited to making explicit estimates.

A natural isomorphism between the two monoid-theoretic structures is applied to relate

- the multiplicative structure of F_{mod} to the additive structure of F_{mod},
- the multiplicative structure of F_{mod} to the quotient monoid $O^{\times}/(\text{roots of unity})$ equipped with the action of the local absolute Galois group,
- the monoid generated by the formal collection $\{\underline{\underline{q}}^{m^2}\}_{1 \leqslant m \leqslant (l-1)/2}$ of theta-values to the quotient monoid $O^{\times}/(\text{roots of unity})$ equipped with the action of the local absolute Galois group.

[45] Relative to the analogy with p-adic Teichmuller theory, see 2.14 and the references therein, IUT corresponds to considering the derivative of the canonical Frobenius lifting, which, in turn, corresponds, relative to the analogy with the classical complex case, to the hyperbolic geometry of the upper half-plane used in the Bogomolov proof. See also Rk 2.3.4 of [31]-IV and [36] for more on this.

[46] When working on IUT, its author was not familiar with the Bogomolov proof.

2.11. **The main theorem of IUT.** Define an idele $q_E \in \mathbb{A}_F$: its components at the nonarchimedean elements of V_F of *odd* residue characteristic[47] where E_F has bad reduction are taken to be the local q-parameters; its components at the other valuations of F are taken to be 1. Compare with the definition of the idele q_{E_F} in 2.2.

Consider any idele $\mathrm{cond}_E \in \mathbb{A}_F$ whose components at the nonarchimedean elements of V_F of *odd* residue characteristic where E_F has bad reduction are (arbitrary) prime elements of the completion of F at v, and whose components at the other valuations of F are equal to 1. The degree $\deg(\mathrm{cond}_E)$ is well-defined and does not depend on the choice of prime elements. Compare $\deg_F(\mathrm{cond}_E)$ with log of $N(\mathrm{Cond}_{E_F})$ discussed in 1.3.

The main theorem[48] is stated in Cor. 3.12 of [31]-III:

$$-\deg(q_E) \leqslant -\deg(\Theta_E),$$

if the RHS is not $+\infty$. Here $-\deg(\Theta_E)$ is by definition the maximum log-volume of deformations for the theta-data, i.e. the maximum of log-volumes of all images with respect to the indeterminacies (Ind1), (Ind2), (Ind3), where one *takes the average over m ranging from 1 to* $(l-1)/2$ as a consequence of the $\mathbb{F}_l^*$-symmetry.

The log-volume on the LHS, i.e., the negative degree $-\deg(q_E)$, is computed in *two equivalent ways*, using the log-theta-lattice and its data at $(1,0)$ and $(0,0)$, see Fig.I.8 of [31]-III. This is achieved in steps (x), (xi) of the proof of Cor. 3.12 of [31]-III, the second of which takes into account the indeterminacies (Ind1), (Ind2), (Ind3) and produces the bound.

One can view this bound as a consequence of a certain hyperbolicity of a number field equipped with an elliptic curve.

One of the main themes of [31] is the issue of deconstructing and reconstructing the two underlying dimensions of a number field. Examples of deconstructing include

- splittings of various local monoids into unit and value group portions, see §I3 of [30]-III
- separating the $\mathbb{Z}/l\mathbb{Z}$ arising from the l-torsion points of the elliptic curve into the additive $\mathbb{F}_l^{\triangleright\!\!\triangleleft\pm}$-symmetry and the multiplicative $\mathbb{F}_l^*$-symmetry, cf. 2.7
- separating the ring structures of global number fields into their respective underlying additive structures, which may be related directly to log-shells, and their respective underlying multiplicative structures, which may be related directly to monoid-theoretic structures.

The reconstruction procedure uses multiradial algorithms involving log-shells and *exhibits the extent to which the two dismantled combinatorial dimensions cannot be separated from one another by describing the intertwining structure between the two dimensions prior to their separation*. This procedure allows one to estimate the value group portions of various monoids of arithmetic interest in terms of their unit group portions and underlies the proof of the inequality in the main theorem.[49]

While local class field theory is used in IUT, global class field theory is not. It is crucial for IUT to use the full Galois and arithmetic fundamental groups.[50]

2.12. **The application of IUT.** In [31]-IV a further (rather straightforward) computation of $-\deg(\Theta_E)$ is made in Th. 1.10 of [31]-IV (assuming, in addition, that the 15-torsion points of E_F are defined over F). It shows that

$$-\deg(\Theta_E) \leqslant a(l) - b(l)\deg(q_E)$$

[47] the main reason for this restriction comes from the use of theta-functions, see Rk 1.10.6 of [31]-IV

[48] $-\deg(q_E)$ equals $-2l|\log(\underline{\underline{q}})|$, while $-\deg(\Theta_E)$ equals $-2l|\log(\underline{\underline{\Theta}})|$ in [31]-III

[49] for more on this one can read Rk 3.12.2 of [31]-III

[50] Compare with the situation in Bogomolov's birational anabelian geometry program for higher dimensional varieties over an algebraic closure of finite field where the use of $G/[G,[G,G]]$ is enough, cf. [5].

where $a(l) > 1$ depends on l, $|F_{\mathrm{mod}} : \mathbb{Q}|$, $\deg(\mathrm{cond}_E) + \deg(\delta_{F/\mathbb{Q}})$, while $b(l) > 1$ is a function of l which does *not* depend on E_F and F.[51]

In the proof one uses the previous theory and the important fact that all the indeterminacies (Ind1), (Ind2), (Ind3) have their range inside the log-shell. Modulo this, the computation of $-\deg(\Theta_E)$ in Th. 1.10 of [31]-IV is essentially completely local, and the local computations are only nontrivial at the nonarchimedean places; the only global aspect of the computation consists of a certain density computation involving the prime number theorem.

Thus, together with the main theorem of IUT, this gives the bound $\deg(q_E) \leqslant a(l)(b(l)-1)^{-1}$. In precise terms,

$$\frac{1}{6}\deg(q_E) \leqslant \left(1 + \frac{2^4 5 |F_{\mathrm{mod}} : \mathbb{Q}|}{l}\right)\left(\deg(\mathrm{cond}_E) + \deg(\delta_{F/\mathbb{Q}})\right) + 2^{14}3^3 5^2 |F_{\mathrm{mod}} : \mathbb{Q}| l + c_\circ,$$

where $c_\circ > 0$ comes from the prime number theorem (over $\mathbb{Q}$) and does not depend on E and F, $\delta_{F/\mathbb{Q}}$ is the (absolute) different of F.

These computations in the proof of Th. 1.10 of [31]-IV were already essentially known to Mochizuki around the year 2000, and an appropriate framework to justify them is provided by IUT, cf. Rk 1.10.1 of [31]-IV.

Then in Cor. 2.2 of [31]-IV one chooses the prime l in the interval $(\sqrt{\deg(q_E)}, 5c_*\sqrt{\deg(q_E)}\log(c_*\deg(q_E)))$ where $c_* = 2^{13}3^3 5 |F_{\mathrm{mod}} : \mathbb{Q}|$, to derive the required bound on $\frac{1}{6}\deg(q_E)$. So, to some degree we already get close to the proof of the Szpiro inequality. Note that here the ε-term in the Szpiro inequality is given an essentially non-archimedean interpretation, modulo various global data and an application of the archimedean estimate given by the prime number theorem.

Using a generalisation of the Belyi map obtained in [25], the Vojta conjecture in 1.3 *over any number field* is proved in [29] to be equivalent to the Vojta conjecture on compactly bounded subsets of $\mathbb{P}^1(\mathbb{Q}^{\mathrm{alg}})$ for $\mathbb{P}^1$ over $\mathbb{Q}$ minus three points $0, 1, \infty$.[52] The use of noncritical Belyi maps in §2 of [31]-IV involves, via the application of [29], the product formula.

Using all this, finally, one deduces the Vojta conjecture (e) of 1.3 (and therefore the conjectures (a), (b), (c) (d) of 1.3 as well), which correspond to Cor. 2.3 of [31]-IV, from Cor. 2.2 of [31]-IV.

Among potential developments and further applications of IUT I will mention one which is asked about by many mathematicians. It is well known that the abc inequality implies that there exists a positive integer n_0 such that the Fermat equation with exponent n does not have positive integer solutions for any $n \geqslant n_0$. In order to make n_0 explicit and hence ideally derive a very different alternative proof of the Wiles–Fermat theorem, one needs to make explicit the constants in the proof of Cor. 2.2 of [31]-IV and to explicitly compute the noncritical Belyi maps which show up in [29]. The latter is currently out of reach. Alternatively, one can try to work with the Frey curve and the Szpiro inequality. Here the main problem is that over $\mathbb{Q}$ one needs bounds on the numbers n_v (see 2.2) associated to *all* the valuations v of the number field $\mathbb{Q}$ except *at most one* (so that one can apply the product formula). However, at the present time, the bounds on these numbers n_v that one obtains from IUT (i.e., from Th. 1.10 of [31]-IV) are not available for *two* valuations of $\mathbb{Q}$, namely, the prime 2 and the archimedean valuation.

[51] Cor. 3.12 of [31]-III supplies the double inequality $-\deg(q_E) \leqslant -\deg(\Theta_E) \leqslant C_\Theta \deg(q_E)$, provided $-\deg(\Theta_E)$ is finite. The constant C_Θ is explicitly computed in Th. 1.10 of [31]-IV. Substituting its value gives the displayed inequality.

[52] See also footnote 15. This reduction allows one to care relatively less about the archimedean data. I think that one can say, to some extent, that in IUT, instead of dealing with the archimedean data aspects of the Szpiro conjectured inequality, by using, say, analytic number theory, which is typically non-scheme-theoretic, one, in effect, moves the centre of activity to the nonarchimedean data, by applying the product formula; the resulting theory is necessarily non-scheme-theoretic.

2.13. **More theorems, objects and concepts of IUT.** Some mathematicians are interested in seeing statements of a large number of theorems in survey texts. As far as IUT and these notes are concerned, this wish is difficult to satisfy, since many central theorems of IUT are of an algorithmic nature, and their statements occupy a lot of space. For example, statements of key theorems in the introductions of IUT papers, i.e. Th. A in [31]-I, Th. A and B in [31]-II and Th. A in [31]-III, occupy 60 lines on average.

My recommendation to readers of these notes who are interested in seeing more theorems is to read the introductions of [28], [30]-III, [31]-I-III, which contain detailed statements of the main theorems and related definitions.

The description of IUT in the previous subsections is a quite simplified one. In particular, I have not written much about the categorical geometric framework developed in IUT and related papers, which underlies the proof of the main theorem of IUT.

Further concepts and methods used in IUT and not discussed above include

- ◇ the concept and theory of frobenioids, cf. [27] I-II (see footnotes 23 and 38, and the examples in 2.10)
- ◇ the concept of arithmetical holomorphy immune to the logarithm, cf. [30]-III
- ◇ the concept of a global multiplicative subspace, cf. [31]-I
- ◇ $\Theta^{\pm\mathrm{ell}}$NF-Hodge-theatres, cf. [31]-I (see footnote 38)
- ◇ profinite conjugacy and tempered conjugacy, cf. [26], [31]-I
- ◇ Belyi cuspidalisation, elliptic cuspidalisation, cf. [30].

2.14. **Analogies and relations between IUT and other theories.** There are many analogies between IUT and p-adic Teichmüller theory (and some analogies with complex Teichmüller theory) which are well described in [32], [33] and in §I4 of [31]-I.

There are certain analogies between IUT and p-adic Hodge theory (which is applied in the proofs of mono-anabelian geometry). For example, the local and global functoriality of absolute anabelian algorithms corresponds to some degree to compatible local isomorphisms between Galois cohomology modules in p-adic Hodge theory, see e.g. Fig.4.2 of [33]. The main ingredients of a frobenioid [27] are reminiscent of the theory of the ring B_{crys} in p-adic Hodge theory.

Hodge–Arakelov theory [23] is not formally used in [31], but some of its ideas and expectations motivate key concepts and objects of [31]; for more on this see [32], [33]. IUT can be viewed as a mathematical justification and background for the realisation of a key idea from [23] concerning a possible approach to establishing the Vojta conjecture, see 2.12.

A number of aspects of the theory of [8] can be viewed as abelian ancestors of certain aspects of IUT, see Rk 2.3.3 of [31]-IV.

Relations with class field theory, inverse Galois theory and anabelian geometry have already been discussed.

The following relations and analogies between IUT and other theories are not used in [31].

IUT works with elliptic curves and related hyperbolic curves over number fields, and it is crucial that they are treated as *two-dimensional* objects. Of course, elliptic curves over number fields can be studied by many methods. In particular, two-dimensional class field theory and adelic geometry and analysis also treat them as two-dimensional objects, cf. [9]. The latter theory studies the zeta function of a surface, geometric or arithmetic. It provides an efficient tool to study three fundamental problems concerning elliptic curves over number fields, which are different from the arithmetic conjectures addressed by IUT. While IUT works with the full Galois and arithmetic fundamental groups, [9] is a commutative theory that is closely connected to abelian Galois groups of two-dimensional fields. Similarly to the two types of symmetry in IUT, geometric-additive and arithmetic-multiplicative, see 2.7, there are two types of symmetry, one additive for geometric

two-dimensional adeles and another symmetry is used for a computation of a two-dimensional zeta integral on multiplicative analytic two-dimensional adeles on surfaces. These two types of adelic symmetry play a fundamental role in [9]. The analytic adelic structure is highly non-scheme-theoretical. In fact, a version if the morphism of local monoid-theoretic structures mentioned at the beginning of 2.7 already showed up in first papers of two-dimensional adelic analysis in 2001.

There are other analogies between Hodge–Arakelov theory of [23] and [9] which led me in May 2012 to the study of the former. The nonarchimedean theta-functions are related to the complex theta-function $\theta(z,\tau)$, as mentioned in 2.5. The Green function for a proper regular model $\mathscr{E}$ of an elliptic curve over a number field is closely related with $\theta(z,\tau)$. On the other hand, the real variable function $\theta(0,ix)$ in x has an adelic interpretation as the integral over $\mathbb{Q}$ of the eigenfunction $\otimes \mathrm{char}_{\mathbb{Z}_p}(x) \otimes \exp(-x^2/2)$ of an adelic Fourier transform with eigenvalue 1 (*char* is the characteristic function), and the Fourier transform, which in this case is called the Mellin transform, of $\theta(0,ix)-1$ is the completed zeta function. Generalisations of these properties play a crucial role in two-dimensional adelic analysis and geometry on $\mathscr{E}$; there is a two-dimensional analogue of $\mathrm{char}_{\mathbb{Z}_p}$ on each singular fibre that takes into account the number of components in the singular fibre, and the zeta integral computation gives a two-dimensional formula for the norm of the minimal discriminant and conductor of the elliptic curve, [9]. The texts [32], [33] and papers of IUT present certain analogies between IUT and the computation of the classical Gaussian integral, and similar analogies exist also between the computation of the Gaussian integral and the computation of the zeta integral in [9].

Two-dimensional adelic analysis and geometry in its current form [9] deals with abelian aspects and does not directly use one-dimensional nonabelian aspects of the Langlands programme. There are many relations between the two theories and also nonabelian versions of [9], to be developed, are related to two-dimensional versions of the programme. At the moment we know little about relations between IUT and nonabelian representation-theoretic aspects of the Langlands programme and their applications to diophantine geometry, see the final portion of §I5 of [31]-I. I expect that more links between the two theories will eventually be found, and, in particular, that the two-dimensional adelic theory of [9] and its nonabelian extensions can serve as a bridge between them.

The algorithmic feature of many theorems of IUT is an interesting aspect. See also 3.2 for the need for a new language to possibly better describe the objects, concepts and results of IUT.

Section 3 of [31]-IV deals with the language of species, naturally associated to IUT. The material of this section has a certain affinity with model theory; for a textbook on the latter see e.g. [41]. In applications of model theory one observes or establishes the same model-theoretic-geometric pattern, typically for stable theories, between a theory T and a distinct theory T'; this common type thus allows one to verify difficult results concerning T' by means of some relatively easy verification concerning T, i.e., to transfer aspects of T to T'. The existing applications of model theory, at least when one deals with formal (first-order) theories, do not involve situations where $T = T'$.[53] IUT studies the case where $T = T'$; this corresponds to the two equivalent ways for computing $-\deg(q_E)$ mentioned in 2.11, see also Fig. I.8 of [31]-III. In this respect, IUT is an interesting object of study from the point of view of model theory.

The use of Galois groups and arithmetic fundamental groups makes IUT very distinct from any other ongoing work on such fundamental issues in mathematics as geometry over $\mathbb{F}_1$, a nontrivial product with itself of an enhanced version of $\mathrm{Spec}(\mathbb{Z})$, analytic geometry over $\mathbb{Z}$, etc., and the possible applications of such notions to the deepest open problems. For two analogies between aspects of IUT and geometry over $\mathbb{F}_1$, see Rk 5.10.2

[53] More generally, in some applications of model theory, e.g. to generalised integration theories, one proves that the same pattern holds for fields of any characteristic

(iii) of [30]-III and Rk 3.12.4 (iii) of [31]-III. Even though it is too early to say, it is natural to expect many connections between IUT and such ongoing work.

There are several well known conjectural approaches to deep properties of arithmetic objects where one wishes to have an arithmetic analogue of a theory which works well in the geometric setting. IUT provides such an arithmetic analogue in the special circumstances related to the arithmetic conjectures of 1.3. A very interesting question is whether some of the mechanisms of IUT could be generalised and extended in order to help to produce new instances of such arithmetic analogues of geometric theories.

One may ask about possible illustrations for arithmetic deformation theory. In my personal opinion, this one[54] is interesting from the point of view of depicting such important aspects of IUT as symmetry, synchronisation, discrete approximation and the role of the number 6.[55]

3. Studying IUT and related aspects

3.1. **On the verification of IUT.** Updated versions and the history of changes of papers related to IUT are available on Sh. Mochizuki's homepage. Some of the changes apply available resources of IUT in a stronger form, in particular addressing analytic number theory remarks made in the autumn of 2012 by Dimitrov and Venkatesh.

G. Yamashita[56] was the first to study IUT and the related papers intensively. He was followed by M. Saïdi and Yu. Hoshi. The changes in the papers of IUT and the prerequisites take into account hundreds of comments from Yamashita, over a hundred comments from Saïdi and several dozens of comments from Hoshi. None of these changes is of a major character.

There are two issues. One is an issue of verification of absence of logical problems in the texts of IUT. As of the time of writing of this text, [31]-I-III and the prerequisites have been checked by mathematicians different from the author 12 times, and [31]-IV has been checked 7 times.[57] Two reports on the verification of IUT, [34] and [35], present impressively vast efforts on the verification of IUT and include many more details. The second issue is of digestion of the theory and its potential simplification. This is likely to take more time, since IUT goes substantially outside the realm of conventional arithmetic geometry.

Numerous activities have been organised at RIMS and elsewhere; participants of cycles of lectures included many mathematicians. A two week workshop on IUT and its developments was held at RIMS in March 2015.[58]

---

[54] The illustration of https://www.maths.nottingham.ac.uk/personal/ibf/graphene-lattice.pptx was presented during a talk of L. Eaves at the Opening Event of the new Molecular Beam Epitaxy Facility for the growth of graphene and boron nitride layers, University of Nottingham, January 2015.

[55] In IUT, the two combinatorial dimensions of a ring, which are often related to two ring-theoretic dimensions (one of which is geometric, the other arithmetic), play a central role. These two dimensions are reminiscent of the two parameters (one of which is related to electricity, the other to magnetism) which are employed in a subtle fashion in the study of graphene to establish a certain important synchronisation for hexagonal lattices.

[56] Three months prior to my planned visit to RIMS in September 2012, I arranged a meeting with Sh. Mochizuki to discuss his theory [23]. After my meeting with Sh. Mochizuki on September 15 at RIMS, which naturally concentrated on IUT, I met with G. Yamashita (who was a postdoc in Nottingham in 2008-2010) and supported his intention to learn and scrutinise the theory when he told me he had already decided to study IUT after receiving my email about IUT on September 1.

[57] G. Hardy: "I have myself always thought of a mathematician as in the first instance an observer, a man who gazes at a distant range of mountains and notes down his observations ... If he wishes someone else to see it, he points to it ... When his pupil also sees it, the proof is finished", p. 598 of vol. 7 of [14].

[58] RIMS Joint Research Workshop: On the verification and further development of inter-universal Teichmüller theory, March 2015, its materials are available from http://www.kurims.kyoto-u.ac.jp/~motizuki/research-english.html

A CMI workshop[59] on IUT will be held in December 2015 in Oxford, and an international conference on IUT and further developments will be organised in Kyoto in July 2016.

As with every innovative theory and even more in this case, whatever is the previous experience of a mathematician, she or he is a student with regard to IUT, and the only way to gain a knowledge of it is to work with its texts. See the foreword of this paper, and the next subsection for some advice on how to study and an estimate of associated time investment.

3.2. **Entrances to IUT.** The number of pages to read and the complexity of this fascinating theory are vast. This may be partially related to the absence of a new language best suited to describing the novel mathematics of IUT.

Initially I found even the review papers [32] and [33] and introductions of IUT papers difficult to understand. The situation improved after a list of the main ideas and methods of IUT revealed the central place of [30]-III and [28]. Reading [30]-III was very useful for my study. Following this single paper helped me to gradually see and appreciate the need for approximately half of the new mathematical concepts and structures in IUT.

Now I will describe possible entries to the theory.

For classical anabelian geometry, if needed, first read Ch.4 of [45] and [13] and also have a look at [42].

The following papers and theories can be read prior to the study of IUT:

- the Bogomolov proof of the geometric version of the Szpiro inequality (see 1.3 and footnote 45), which involves geometric considerations that are substantially reminiscent of the geometry that underlies the Hodge theatres of [31]-I, cf. sect. 5.3 of [1], [4], [50], see also footnote 45
- the classical theory of the functional equation of the theta-function, as discussed, for instance in §1.7.5 of [7], which was one important motivation for the development of the theory of [31]-II-III, see also [37] for more on the archimedean theta-function
- the classical theory of moduli of ordinary elliptic curves in positive characteristic and the related structure of the Hecke correspondence (i.e. T_p) in positive characteristic, which is also substantially reminiscent of the geometry that underlies the Hodge theatres of [31]-I.

For IUT: first read §1–2 of [30]-III (and any previous relevant papers) and [28], and then the papers of [31], consulting [27] when necessary, as well as [25] and [29], which are used in [31]-IV.

Category theorists and algebraists may prefer to start with a reading of [27] and [24].

3.3. **The work of Shinichi Mochizuki.** The mathematical vision and perseverance of the author of IUT during 20 years of work on it is most admirable and is a sample to follow.

A valuable addition to this is his investment of time and effort in answering questions about his work and explaining and discussing its parts, via email communication or skype talks and during numerous meetings and seminars at RIMS.

This theory is so radically different from anything that came before it that it is natural to ask whether it will induce a paradigm shift, and also how it may change the way one can approach mathematical research. The reconstruction algorithm-theoretic approach of [31]-I-III, as well as of [30]-III, [28], contains elements that are radically different from the usual approach to proving theorems, and hence from the usual approach to writing mathematical papers. To some degree, IUT may be thought of as a sort of meta-structure which acts on appropriate parts of conventional scheme-theoretic arithmetic geometry. In doing so, it allows one to explicate,

[59] https://www.maths.nottingham.ac.uk/personal/ibf/files/symcor.iut.html

with relative ease, phenomena (such as the Vojta conjecture) that seemed inaccessible via existing mathematical theories.

Knowing what one can achieve if one works persistently on a long-term goal provides one with an optimistic hope that other difficult challenges might be solved as the result of long-term resolute innovative work.

3.4. **Related issues.** It is clear how crucial long-term work is for real breakthroughs in mathematics. Questions arise such as how to increase the number of researchers able to work for a long time on fundamental problems so sedulously and successfully and what should be the amount of support to this strategically important type of research work.

An opinion of R. Langlands on current trends about supporting long-term fundamental research work can be heard during the 52nd minute of his video lecture [20].

Some roots of the decline of support to long-term fundamental work, such as the shortsighted race to higher number of publications and higher citation index, which often results in pressure to produce short-term work that consists essentially of minor improvements to known results, originate from causes external to the mathematical community. To do well in their academic career, young researchers are very often pushed to go along this path which typically implies a very narrow specialisation. The latter leads to the emphasis on technical perfection as opposite to innovation and on presentation rather than substance of work. Following this path eventually makes it more difficult to think in broader terms, to learn new concepts, to develop in new directions. Lack of inventiveness, more widely spread imitation, very pragmatic attitudes to what and when to study in mathematics, lack of genuine enthusiasm to study new theories, fear to stand alone in scientific endeavour, fear to look too far away are associated issues. Some roots, such as the unnecessarily strong emphasis on concrete applications[60], originate from within the mathematical community.

There is an issue about attitudes of number theorists towards the study of IUT and their unusually sluggish response. Reasons for this are related to the topics discussed in the third paragraph of 3.3 and in the previous paragraph. It seems that the number theory community is suffering from the problems listed there even more than other mathematical communities.

Acknowledgements. I am most grateful to Shinichi Mochizuki for many interesting and often fascinating discussions and for his answers to my numerous questions, as well as for his valuable comments and remarks on preliminary drafts of this text. I am thankful to Akio Tamagawa for supporting my visits to RIMS in September 2012 and December 2014. I am thankful to Go Yamashita for answering my questions on IUT prior to my second visit to RIMS, as well as to him and Yuichiro Hoshi for answering my specialised questions during my visit. I am very grateful to Fedor Bogomolov for highly interesting discussions on his work. Work on this text was partially supported by University of Nottingham and EPSRC programme grant EP/M024830.

REFERENCES

[1] J. AMOROS, F. BOGOMOLOV, L. KATZARKOV, T. PANTEV, Symplectic Lefschetz fibrations with arbitrary fundamental groups, *J. Diff. Geometry* 54(2000) 489–545, available from http://arxiv.org/abs/math/9810042

[2] Arithmetic geometry, G. Cornell, J.H. Silverman (eds.), Springer 1986.

[3] G. V. BELYI, On Galois extensions of a maximal cyclotomic field, *Izv. Akad. Nauk SSSR Ser. Mat.* 43:2 (1979), 269–276; English transl. in *Math. USSR- Izv.* 14 (1980), 247–256.

[4] F. BOGOMOLOV, L. KATZARKOV, T. PANTEV, Hyperelliptic Szpiro inequalities, *J. Diff. Geometry* 61(2002) 51–80, available from http://arxiv.org/abs/math/0106212

[60] recall the very topical words of Grothendieck in this respect on p.1 of [13]

[5] F. BOGOMOLOV, YU. TSCHINKEL, Galois theory and projective geometry, *Comm. Pure and Applied Math.*, 66, no. 9, 1335–1359, (2013); available from http://www.math.nyu.edu/~tschinke/papers/yuri/11cpam/cpam10.pdf

[6] E. BOMBIERI, W. GUBLER, Heights in diophantine geometry, CUP 2006.

[7] H. DYM, H.P. MCKEAN, Fourier series and integrals, Academic Press 1972.

[8] G. FALTINGS, Endlichkeitssätze für Abelschen Varietäten über Zahlkörpern, *Invent. Math.* 73(1983), 349–366.

[9] I. FESENKO, Adelic approach to the zeta function of arithmetic schemes in dimension two, *Moscow Math. J.* 8 (2008), 273–317, available from https://www.maths.nottingham.ac.uk/personal/ibf/ada.pdf

[10] I.B. FESENKO, S.V. VOSTOKOV, Local fields and their extensions, 2nd extended ed., AMS 2002, available from https://www.maths.nottingham.ac.uk/personal/ibf/book/book.html

[11] M. GROMOV, Hyperbolic manifolds (according to Thurston and Jorgensen), In Bourbaki Seminar, Vol. 1979/80, Lecture Notes Math. 842, Springer 1981, pp. 40–53.

[12] A. GROTHENDIECK, Esquisse d'un programme, 1983, in P. Lochak, L. Schneps, Geometric Galois actions 1, *LMS Lect. Note Ser.* 242, CUP 1997, available from http://webusers.imj-prg.fr/~leila.schneps/grothendieckcircle/EsquisseFr.pdf; English transl. is available from http://webusers.imj-prg.fr/~leila.schneps/grothendieckcircle/EsquisseEng.pdf

[13] A. GROTHENDIECK, anabelian letter to G. Faltings, June 1983, in P. Lochak, L. Schneps, Geometric Galois actions 1, *LMS Lect. Note Ser.* 242, CUP 1997, available from http://webusers.imj-prg.fr/~leila.schneps/grothendieckcircle/Letters/GanF.pdf; English transl. is available from http://webusers.imj-prg.fr/~leila.schneps/grothendieckcircle/Letters/GtoF.pdf

[14] G. HARDY, Collected papers, OUP, 1966–1979.

[15] M. HINDRY, J. SILVERMAN, Diophantine geometry: an introduction, Springer 2000.

[16] YU. HOSHI, Existence of nongeometric pro-p Galois sections of hyperbolic curves, *Publ. RIMS* 46 (2010), 829–848, available from http://www.kurims.kyoto-u.ac.jp/~yuichiro/existence_of_nongeometric_pro-p_galois_sections.pdf

[17] YU. HOSHI, Mono-anabelian reconstruction of number fields, *RIMS preprint* 1819 (2015), available from http://www.kurims.kyoto-u.ac.jp/~yuichiro/rims1819.pdf

[18] YU. HOSHI, SH. MOCHIZUKI, Topics surrounding the combinatorial anabelian geometry of hyperbolic curves IV: discreteness and sections, RIMS Preprint 1788, September 2013, available from http://www.kurims.kyoto-u.ac.jp/~motizuki/Combinatorial%20Anabelian%20Topics%20IV.pdf

[19] M. KIM, A remark on fundamental groups and effective diophantine methods for hyperbolic curves, in Number theory, analysis and geometry – in memory of S.Lang, Springer 2010, available from http://people.maths.ox.ac.uk/kimm/papers/effective.pdf

[20] R. LANGLANDS, Problems in the theory of automorphic forms: 45 years later, video lectures at Nottingham–Oxford conference on symmetries and correspondences, July 2014, Oxford Univ., available from https://www.maths.nottingham.ac.uk/personal/ibf/files/S&C-schedule.html

[21] G. MALLE, B.H. MATZAT, Inverse Galois theory, Springer 1999.

[22] J. MILNE, Arithmetic duality theorems, 2nd revised ed., BookSurge, 2004 and 2006, available from http://www.jmilne.org/math/Books/ADTnot.pdf

[23] SH. MOCHIZUKI, A survey of the Hodge–Arakelov theory of elliptic curves I, in Proc. of Symp. Pure Math. 70, AMS (2002), 533–569; II, in Algebraic Geometry 2000, Azumino, Adv. Stud. Pure Math. 36, Math. Soc. Japan (2002), 81–114, available with comments from http://www.kurims.kyoto-u.ac.jp/~motizuki/papers-english.html

[24] SH. MOCHIZUKI, The geometry of anabelioids, *Publ. Res. Inst. Math. Sci.* 40 (2004), 819–881, available with comments from http://www.kurims.kyoto-u.ac.jp/~motizuki/papers-english.html

[25] SH. MOCHIZUKI, Noncritical Belyi maps, *Math. J. Okayama Univ.* 46 (2004), 105–113, available with comments from http://www.kurims.kyoto-u.ac.jp/~motizuki/papers-english.html

[26] SH. MOCHIZUKI, Semi-graphs of anabelioids, *Publ. Res. Inst. Math. Sci.* 42 (2006), 221–322, available with comments from http://www.kurims.kyoto-u.ac.jp/~motizuki/papers-english.html

[27] SH. MOCHIZUKI, The geometry of frobenioids I: The General theory, *Kyushu J. Math.* 62 (2008), 293–400; II: Poly-Frobenioids, *Kyushu J. Math.* 62 (2008), 401–460, available with comments from http://www.kurims.kyoto-u.ac.jp/~motizuki/papers-english.html

[28] SH. MOCHIZUKI, The étale theta function and its frobenioid-theoretic manifestations, *Publ. Res. Inst. Math. Sci.* 45 (2009), 227–349, available with comments from http://www.kurims.kyoto-u.ac.jp/~motizuki/papers-english.html

[29] SH. MOCHIZUKI, Arithmetic elliptic curves in general position, *Math. J. Okayama Univ.* 52 (2010),1–28, available with comments from http://www.kurims.kyoto-u.ac.jp/~motizuki/papers-english.html

[30] SH. MOCHIZUKI, Topics in absolute anabelian geometry I: Generalities, *J. Math. Sci. Univ. Tokyo* 19 (2012), 139–242; II: Decomposition groups and endomorphisms, *J. Math. Sci. Univ. Tokyo* 20 (2013), 171–269; III: Global reconstruction algorithms, J. Math. Sci. Univ. Tokyo 22 (2015), 939–1156, available with comments from http://www.kurims.kyoto-u.ac.jp/~motizuki/papers-english.html

[31] SH. MOCHIZUKI, Inter-universal Teichmüller theory I: Constructions of Hodge theaters, preprint 2012–2015, II: Hodge-Arakelov-theoretic evaluation, preprint 2012–2015; III: Canonical splittings of the log-theta-lattice, preprint 2012–2015; IV: Log-volume computations and set-theoretic foundations, preprint 2012–2015, available from http://www.kurims.kyoto-u.ac.jp/~motizuki/papers-english.html

[32] SH. MOCHIZUKI, Invitation to inter-universal Teichmüller theory (lecture note version), available from http://www.kurims.kyoto-u.ac.jp/~motizuki/Invitation%20to%20Inter-universal%20Teichmuller%20Theory%20(Lecture%20Note%20Version).pdf

[33] SH. MOCHIZUKI, A panoramic overview of inter-universal Teichmüller theory, in Algebraic number theory and related topics 2012, RIMS Kokyuroku Bessatsu B51, RIMS, Kyoto (2014), 301–345, available from http://www.kurims.kyoto-u.ac.jp/~motizuki/Panoramic%20Overview%20of%20Inter-universal%20Teichmuller%20Theory.pdf

[34] SH. MOCHIZUKI, On the verification of inter-universal Teichmüller theory: a progress report (as of December 2013), available from http://www.kurims.kyoto-u.ac.jp/~motizuki/IUTeich%20Verification%20Report%202013-12.pdf

[35] SH. MOCHIZUKI, On the verification of inter-universal Teichmüller theory: a progress report (as of December 2014), available from http://www.kurims.kyoto-u.ac.jp/~motizuki/IUTeich%20Verification%20Report%202014-12.pdf

[36] SH. MOCHIZUKI, Bogomolov's proof of the geometric version of the Szpiro conjecture from the point of view of inter-universal Teichmüller theory, available from http://www.kurims.kyoto-u.ac.jp/~motizuki/Bogomolov%20from%20the%20Point%20of%20View%20of%20Inter-universal%20Teichmuller%20Theory.pdf

[37] D. MUMFORD, Tata lectures on theta, Vols. I–II and III, Birkhäuser, 1983 and 1991.

[38] D. MUMFORD, An analytic construction of degenerating abelian varieties over complete rings, appendix to G. Faltings, C.-L. Chai, Degenerations of abelian varieties, Springer 1990.

[39] J. NEUKIRCH, Algebraic number theory, Springer 1999, available from http://www.mathi.uni-heidelberg.de/~schmidt/NSW2e/index.html and the list of corrections available from http://www.mathi.uni-heidelberg.de/~schmidt/NSW2e/errata-nsw2e.pdf

[40] J. NEUKIRCH, A. SCHMIDT, K. WINGBERG, Cohomology of number fields, corr. 2nd ed., Springer 2008, available from http://www.mathi.uni-heidelberg.de/~schmidt/NSW2e/index.html and the list of corrections available from http://www.mathi.uni-heidelberg.de/~schmidt/NSW2e/errata-nsw2e.pdf

[41] B. POIZAT, A course in model theory, Springer 2000 (translated into English from the original French edition published by the author in 1985).

[42] F. POP, Lectures on anabelian phenomena in geometry and arithmetic (December 2010), available from http://math-proxy.sas.upenn.edu/~pop/Research/files-Res/AnabPhen_20Dec10.pdf

[43] A. ROBERT, Elliptic curves, Lect. Notes Math. 326, Springer 1973.

[44] J. SILVERMAN, Advanced topics in the arithmetic of elliptic curves, Springer 1994.

[45] T. SZAMUELY, Galois groups and fundamental groups, CUP 2009, corrections are available from http://www.renyi.hu/~szamuely/erratafg.pdf

[46] J. TATE, A review of non-archimedean elliptic functions, available from https://www.ma.utexas.edu/users/voloch/Ellnotes/nonarch-ams.pdf

[47] P. VOJTA, A more general abc conjecture, *Int. Math. Res. Not.*, 21 (1998), 1103–1116, available from http://arxiv.org/pdf/math/9806171v1.pdf

[48] P. VOJTA, Diophantine inequalities and Arakelov theory, Appendix of S. Lang, Introduction to Arakelov theory, Springer 1988.

[49] M. WALDSCHMIDT, On the abc conjecture and some of its consequences, March 2013, available from http://webusers.imj-prg.fr/~michel.waldschmidt/articles/pdf/abcLahore2013VI.pdf

[50] SH. ZHANG, Geometry of algebraic points, In First Intern. Congr. Chinese Mathematicians (Beijing, 1998), 185–198, AMS/IP Stud.Adv.Math. 20 (2001), available from https://web.math.princeton.edu/~shouwu/publications/iccm98.pdf