Inter-universal Teichmüller Theory as an Anabelian Gateway to Diophantine Geometry and Analytic Number Theory

Shinichi Mochizuki

(joint work with Yuichiro Hoshi, Arata Minamide, Shota Tsujimura, and Go Yamashita)

1. Overview via a famous quote of Poincaré

One question that is frequently asked concerning inter-universal Teichmüller theory (IUT) is the following: Why/how does IUT allow one to apply **anabelian geometry** to prove **diophantine** results? In this talk, we addressed this question by giving an *overview of various aspects of IUT*, many of which may be regarded as *striking examples* of the famous quote of *Poincaré* to the effect that "**mathematics is the art of giving the same name to different things**" — which was apparently *originally motivated* by various observations on the part of Poincaré concerning certain remarkable similarities between *transformation group symmetries* of modular functions such as *theta functions*, on the one hand, and *symmetry groups* of the *hyperbolic geometry* of the *upper half-plane*, on the other — all of which are *closely related to IUT* (cf. [EssLgc], §1.5; the discussion surrounding (InfH) in [EssLgc], §3.3; [EssLgc], Example 3.3.2). Here, we note that there are (at least) *three ways* in which this quote of *Poincaré* is related to *IUT*: the *original motivation* of Poincaré (mentioned above), the key IUT notions of *coricity/multiradiality* (cf. §2, §3 below), and *new applications* of the *Galois-orbit version of IUT* (cf. §4 below). One important theme in this context consists of the observation that one may acquire a rough *survey-level* understanding of IUT using only a knowledge of such elementary topics as the notions of *rings/fields/groups/monoids* (cf. §2 below; [EssLgc], Example 2.4.8) and the elementary geometry of the *projective line/Riemann sphere/analytic continuation* (cf. §3 below; [EssLgc], Example 2.4.7). A more detailed exposition of IUT may be found in the *survey texts* [Alien], [EssLgc], as well as, of course, in the original papers [IUTch], which are exposed in the *videos/slides* available at [ExHr].

2. The N-th power map and Galois groups as abstract groups

Let R be an *integral domain* (such as $\mathbb{Z} \subseteq \mathbb{Q}$) equipped with the action of a *group* G, $(\mathbb{Z} \ni)\ N \geq 2$. For simplicity, we assume that $N = 1+\cdots+1 \neq 0 \in R$, and that R has *no nontrivial N-th roots of unity.* Write $R^{\triangleright} \subseteq R$ for the *multiplicative monoid* $R \setminus \{0\}$. Then let us observe that the *N-th power map* on $R^{\triangleright}$ determines an *isomorphism of multiplicative monoids* equipped with actions by G, i.e., $G \curvearrowright R^{\triangleright} \xrightarrow{\sim} (R^{\triangleright})^N\ (\subseteq R^{\triangleright}) \curvearrowleft G$, that does *not arise* from a *ring homomorphism*, i.e., is clearly *not compatible* with *addition* (cf. our assumption on N!). Next, let ${}^{\dagger}R$, ${}^{\ddagger}R$ be *two distinct copies* of the integral domain R, equipped with respective actions by *two distinct copies* ${}^{\dagger}G$, ${}^{\ddagger}G$ of the group G. We shall use similar notation for objects with labels "†", "‡" to the previously introduced notation. Then one may use the *isomorphism of multiplicative monoids* arising from the *N-th power map* discussed above to *glue* together

$$^{\dagger}G \curvearrowright {}^{\dagger}R \supseteq ({}^{\dagger}R^{\rhd})^N \quad \stackrel{\sim}{\leftarrow} \quad {}^{\ddagger}R^{\rhd} \subseteq {}^{\ddagger}R \curvearrowleft {}^{\ddagger}G$$

the *ring* $^{\dagger}R$ to the *ring* $^{\ddagger}R$ along the *multiplicative monoid* $({}^{\dagger}R^{\rhd})^N \stackrel{\sim}{\leftarrow} {}^{\ddagger}R^{\rhd}$. This gluing is *compatible* with the respective actions of $^{\dagger}G$, $^{\ddagger}G$ relative to the isomorphism $^{\dagger}G \stackrel{\sim}{\rightarrow} {}^{\ddagger}G$ given by forgetting the labels "†", "‡", but, since the N-th power map is **not compatible** with **addition** (!), this isomorphism $^{\dagger}G \stackrel{\sim}{\rightarrow} {}^{\ddagger}G$ may be regarded either as an isomorphism of (*"coric"*, i.e., *invariant* with respect to the N-th power map) **abstract groups** (cf. the notion of *"inter-universality"*, as discussed in [EssLgc], §3.2, §3.8) or as an isomorphism of groups equipped with actions on certain *multiplicative monoids*, but **not** as an isomorphism of (**"Galois"** — cf. the *classical inner automorphism indeterminacies* of SGA1) groups equipped with actions on *rings/fields*. The problem of *describing (certain portions of the) ring structure* of $^{\dagger}R$ in terms of the *ring structure* of $^{\ddagger}R$ — in a fashion that is *compatible* with the *gluing* and via a *single* algorithm that may be applied to the *common* (cf. *logical AND* $\wedge$*!*) *glued data* to reconstruct *simultaneously* (certain portions of) the ring structures of *both* $^{\dagger}R$ and $^{\ddagger}R$, up to suitable relatively mild *indeterminacies* (cf. the theory of *crystals*!) — seems (at first glance/in general) to be *hopelessly intractable* (cf. the case where $R = \mathbb{Z}$)! (One well-known example may be seen in the situation where, when $N = p$, one works *modulo* p (cf. the point of view of *indeterminacies*, the analogy with *crystals*!), so that there is a *common ring structure* that is *compatible* with the *p-th power map*.) This is precisely what is *achieved in IUT* (cf. the quote of *Poincaré*!) by means of the **multiradial algorithm** for the **Θ-pilot** via **anabelian geometry** (cf. the *abstract groups* $^{\dagger}G$, $^{\ddagger}G$!), the ***p*-adic/complex logarithm** and **theta functions**, and **Kummer theory** (to relate **Frobenius-/étale-like** versions of objects). Thus, in summary, the *multiplicative monoid* and *abstract group* structures (but *not* the ring structures!) are *common* (cf. *"logical AND* $\wedge$*!"*) to †, ‡. On the other hand, once one *deletes* the *labels* "†", "‡" to secure a "common R", one obtains a *meaningless* situation, where the common glued data may be related via "†" *OR "*$\vee$*"* via "‡" to the common R, but *not simultaneously* to both. When $R = \mathbb{Z}$ (or, more generally, the *ring of integers* "$\mathcal{O}_F$" of a number field F — cf. the multiplicative *norm map* $\mathrm{N}_{F/\mathbb{Q}} : F \rightarrow \mathbb{Q}$), one may consider the **"height"** $\log(|x|) \in \mathbb{R}$ for $0 \neq x \in \mathbb{Z}$. Then the *N-th power map* corresponds, after passing to *heights*, to *multiplication by N*; the *multiradial algorithm* corresponds to saying that the height is *unaffected (up to a mild error term!)* by *multiplication by N*, i.e., that the *height is bounded*.

3. Conceptual analogies with the projective line/Riemann sphere

Let k be a *field* (which, in fact, could be taken to be an arbitrary ring), R a *k-algebra*. Denote the *units* of a ring by a superscript "$\times$". Write $\mathbb{A}^1$ for the *affine line* $\mathrm{Spec}\,(k[T])$ over k, $\mathbb{G}_{\mathrm{m}}$ for the open subscheme $\mathrm{Spec}\,(k[T, T^{-1}])$ of $\mathbb{A}^1$ obtained by removing the origin. Recall that the standard coordinate T on $\mathbb{A}^1$ and $\mathbb{G}_{\mathrm{m}}$ determines *natural bijections* $\mathbb{A}^1(R) \stackrel{\sim}{\rightarrow} R$, $\mathbb{G}_{\mathrm{m}}(R) \stackrel{\sim}{\rightarrow} R^{\times}$ that are compatible with the well-known natural structures on $\mathbb{A}^1$ and $\mathbb{G}_{\mathrm{m}}$, respectively, of *ring scheme/(multiplicative) group scheme* over k. Next, write $^{\dagger}\mathbb{A}^1$, $^{\ddagger}\mathbb{A}^1$ for the *k-ring schemes* given by *copies* of $\mathbb{A}^1$ equipped with *labels* "†", "‡". Observe that there exists a *unique isomorphism* of *k-ring schemes* ${}^{\dagger}\mathbb{A}^1 \xrightarrow{\sim} {}^{\ddagger}\mathbb{A}^1$; moreover, there exists a *unique isomorphism* of *k-group schemes* $(-)^{-1} : {}^{\dagger}\mathbb{G}_{\mathrm{m}} \xrightarrow{\sim} {}^{\ddagger}\mathbb{G}_{\mathrm{m}}$ that maps ${}^{\dagger}T \mapsto {}^{\ddagger}T^{-1}$. Note that $(-)^{-1}$ does *not extend* to an isomorphism ${}^{\dagger}\mathbb{A}^1 \xrightarrow{\sim} {}^{\ddagger}\mathbb{A}^1$ and is clearly *not compatible* with the *k-ring scheme structures* of ${}^{\dagger}\mathbb{A}^1$ $(\supseteq {}^{\dagger}\mathbb{G}_{\mathrm{m}})$, ${}^{\ddagger}\mathbb{A}^1$ $(\supseteq {}^{\ddagger}\mathbb{G}_{\mathrm{m}})$. The *standard construction* of the *projective line* $\mathbb{P}^1$ may be understood as the result of *gluing* ${}^{\dagger}\mathbb{A}^1$ to ${}^{\ddagger}\mathbb{A}^1$ along the isomorphism

$$ {}^{\dagger}\mathbb{A}^1 \supseteq {}^{\dagger}\mathbb{G}_{\mathrm{m}} \stackrel{(-)^{-1}}{\longrightarrow} {}^{\ddagger}\mathbb{G}_{\mathrm{m}} \subseteq {}^{\ddagger}\mathbb{A}^1 $$

— i.e., at the level of *R-rational points* ${}^{\dagger}R \supseteq {}^{\dagger}R^{\times} \stackrel{(-)^{-1}}{\longrightarrow} {}^{\ddagger}R^{\times} \subseteq {}^{\ddagger}R$ — where ${}^{\Box}R = {}^{\Box}\mathbb{A}^1(R)$, ${}^{\Box}R^{\times} = {}^{\Box}\mathbb{G}_{\mathrm{m}}(R)$, for $\Box \in \{\dagger, \ddagger\}$ (cf. the *gluing* situation discussed in §2, where "$(-)^{-1}$" corresponds to "$(-)^N$"!). In particular, *relative to this gluing*, we observe that there exists a *single rational function* on the copy of "$\mathbb{G}_{\mathrm{m}}$" that appears in the gluing that is *simultaneously* equal to the rational function ${}^{\dagger}T$ on ${}^{\dagger}\mathbb{A}^1$ *AND* [cf. "$\wedge$"!] to the rational function ${}^{\ddagger}T^{-1}$ on ${}^{\ddagger}\mathbb{A}^1$. Thus, in summary, the standard construction of $\mathbb{P}^1$ may be regarded as consisting of a *gluing* of two *ring schemes* along an *isomorphism* of *multiplicative group schemes* that is *not compatible* with the *ring scheme* structures on either side of the gluing. Here, we observe that if, in the gluing under discussion, one *arbitrarily deletes* the *distinct labels* "†", "‡" (e.g., on the grounds that both ring schemes represent "THE" structure sheaf "$\mathcal{O}_X$" of a k-scheme X!), then the resulting *"gluing without labels"* amounts to a gluing of a *single copy* of $\mathbb{A}^1$ to itself that maps the standard coordinate T on $\mathbb{A}^1$ (regarded, say, as a rational function on $\mathbb{A}^1$) to T^{-1}. That is to say, such a *deletion of labels* (even when restricted to the (abstractly isomorphic) multiplicative monoids ${}^{\dagger}T^{\mathbb{Z}}$, ${}^{\ddagger}T^{\mathbb{Z}}$!) immediately results in a *contradiction* (i.e., since $T \neq T^{-1}$!), unless one passes to some sort of *quotient* of $\mathbb{A}^1$, e.g., by introducing some sort of *indeterminacy*, which amounts to the consideration of some sort of *collection of possibilities* [cf. "$\vee$"!].

When $k = \mathbb{C}$ (i.e., the *complex number field*), one may think of $\mathbb{P}^1$ as the *Riemann sphere* $\mathbb{S}^2$ equipped with the *Fubini-Study metric* and of the gluing under discussion as the gluing, along the *equator* $\mathbb{E}$, of the *northern hemisphere* $\mathbb{H}^+$ to the *southern hemisphere* $\mathbb{H}^-$. Then the above discussion of standard coordinates "${}^{\dagger}T$", "${}^{\ddagger}T$" translates into the following (at first glance, *self-contradictory*!) phenomenon: an *oriented flow* along the *equator* — which may be thought of physically as a sort of *east-to-west wind current* — appears *simultaneously* to be flowing in the *clockwise* direction, from the point of view of $\mathbb{H}^+ \subseteq \mathbb{S}^2$, *AND* in the *counterclockwise* direction, from the point of view of $\mathbb{H}^- \subseteq \mathbb{S}^2$. Indeed, if one *arbitrarily deletes the labels* "+", "−" and *identifies* $\mathbb{H}^-$ with $\mathbb{H}^+$, then one literally obtains a *contradiction*. On the other hand, one may relate $\mathbb{H}^-$ to $\mathbb{H}^+$ (*not* by such an arbitrary deletion of labels (!), but rather) by applying the well-known **metric/geodesic geometry/isometric symmetries** of $\mathbb{S}^2$ — i.e., by considering the *geodesic flow* along *great circles/lines of longitude* — to **represent**, up to a *relatively mild distortion*, the entirety of $\mathbb{S}^2$, i.e., including $\mathbb{H}^- \subseteq \mathbb{S}^2$, as a sort of **deformation/displacement** of $\mathbb{H}^+$ (cf. the point of view of *cartography*!). It is precisely this metric/geodesic/symmetry-based approach that corresponds to the *anabelian geometry*-based *multiradial algorithm for the* Θ*-pilot* in IUT (cf. the analogy discussed in [Alien], §3.1, (iv), (v), as well as in [EssLgc], §3.5, §3.10, between *multiradiality* and *connections/parallel transport/crystals*!).

In this context, it is important to remember that, just like SGA, IUT is *formulated entirely in the framework* of **"ZFCG"** (i.e., ZFC, plus Grothendieck's axiom on the existence of universes), especially when considering various *set-theoretic/foundational* aspects of *"gluing"* operations in IUT (cf. [EssLgc], §1.5, §3.8, §3.9, as well as [EssLgc], §3.10, especially the discussion of *"log-shift adjustment"* in (Stp 7)), such as the following: gluings are performed at the abstract level of *diagrams* (cf. graphs of groups/anabelioids) and are *not* equipped with any *embedding* into some *familiar ambient space* (like a sphere); the *output of reconstruction algorithms* is only well-defined at the level of *objects up to isomorphism* (up to *suitable indeterminacies*), i.e., "types/packages of data" (such as groups, rings, monoids, diagrams, etc.) called *"species"* — one consequence of which is the central importance of *closed loops* in order to obtain *set-theoretic comparisons* that are *not possible at intermediate steps*. Here, we note the importance of working with *"types/packages of data"* (cf., e.g., the *diagrams* referred to above), as opposed to certain particular underlying sets of interest (cf. the classical functoriality of *resolutions* in cohomology, as well as of *algebraic closures* of fields up to *conjugacy indeterminacies* — which become unnecessary, e.g., if one considers *norms*), as well as the importance of working with **"closed loops"** (cf. *norms* in Galois theory; the classical theory of *analytic continuation/Riemann surfaces* — which is reminiscent of the classical *Riemann-Weierstrass* dispute! (cf. [EssLgc], §1.5); the *geodesic completeness/closed geodesics/isometric symmetries* of the sphere).

4. New enhanced versions of IUT and related work in progress

Recent joint work in progress focuses on the *Section Conjecture ("SC")* in anabelian geometry and allows one (cf. [GSCsp]) to reduce, using *"resolution of nonsingularities (RNS)"* (cf. [RNSPM]), together with a result of Stoll, the geometricity of an arbitrary Galois section of a hyperbolic curve over a number field to *local geometricity* at each nonarchimedean prime, together with *3 global conditions*, which correspond, respectively, to *3 new enhanced versions of IUT* that are currently under development. Moreover, this theory of [GSCsp], when combined with other joint work in progress (cf. [AnPf]), has led to substantial progress on the *p-adic SC* that is closely related to the use of *Raynaud-Tamagawa "new-ordinariness"* in the theory of *RNS* (cf. [RNSPM]), and which is noteworthy in that it functions as a sort of *local p-adic analogue of IUT*, via the following analogy: "$\mathrm{Norm}(-) = (-)$" $\longleftrightarrow$ "$N \cdot (-) \approx (-)$" (cf. §2). One such new enhanced version of IUT is the *Galois-orbit version of IUT (GalOrbIUT)*, which implies the following: one of the 3 global conditions mentioned above in the discussion of the *SC* (called *"intersection-finiteness"*), the *nonexistence of Siegel zeroes* of Dirichlet L-functions associated to imaginary quadratic number fields (i.e., by applying the work of Colmez/Granville-Stark/Táfula), and a *numerically stronger* version of the *abc/Szpiro* inequalities. That is to say, we obtain three *a priori different* applications to *anabelian geometry* (the "local-global" SC), *analytic number* *theory* (nonexistence of Siegel zeroes), and *diophantine geometry* (abc/Szpiro inequalities) — a *striking example* of *Poincaré's quote*, i.e., all three are essentially the **same mathematical phenomenon** of **bounding heights**, i.e., **bounding "local denominators"**. Other noteworthy aspects of the *local-global SC* application include the following: it exhibits IUT as "*anabelian geometry* applied to obtain more *anabelian geometry*" (hence is less psychologically/intuitively surprising than the other two applications); it is *technically the most difficult/essential* of the three, i.e., to the extent that the *other two* applications may be thought of, to a substantial extent, as being *"inessential by-products"*; it is similar in spirit to the *historical point of view* (cf., e.g., of Grothendieck's famous "letter to Faltings") that suggests (*without any proof!*) that the SC might imply results in diophantine geometry (such as the Mordell Conjecture). Finally, in this context, it is interesting to recall (cf. [Alien], §3.11, (iii)) that the essential content of *anabelian geometry* may be understood as a sort of **"conceptual translation"** of the *abc inequality*: indeed, just as **anabelian geometry** centers around reconstructing *addition* from *multiplication*, the **abc inequality** may be thought of as a bound on the *height (or "additive size")* of a number by the *conductor (or "multiplicative size")* of the number, i.e., both of these situations exhibit **addition** as being "**dominated** by" **multiplication**. This "conceptual"/"numerical" correspondence is reminiscent of the well-known correspondence between the *conceptual* nature of the *Weil Conjectures* and the corresponding *numerical inequalities* for the number of rational points of a variety over a finite field.

References

[ExHr] Videos/slides available at the following URLs: `https://www.kurims.kyoto-u.ac.jp/~motizuki/ExpHorizIUT21/WS3/ExpHorizIUT21-InvitationIUT-notes.html` ; `https://www.kurims.kyoto-u.ac.jp/~motizuki/ExpHorizIUT21/WS4/ExpHorizIUT21-IUTSummit-notes.html`

[IUTch] S. Mochizuki, *Inter-universal Teichmüller Theory I: Construction of Hodge Theaters*, Publ. Res. Inst. Math. Sci. **57** (2021), 3–207; *II: Hodge-Arakelov-theoretic Evaluation*, Publ. Res. Inst. Math. Sci. **57** (2021), 209–401; *III: Canonical Splittings of the Log-theta-lattice*, Publ. Res. Inst. Math. Sci. **57** (2021), 403–626; *IV: Log-volume Computations and Set-theoretic Foundations*, Publ. Res. Inst. Math. Sci. **57** (2021), 627–723.

[Alien] S. Mochizuki, *The Mathematics of Mutually Alien Copies: from Gaussian Integrals to Inter-universal Teichmüller Theory*, Inter-universal Teichmüller Theory Summit 2016, RIMS Kōkyūroku Bessatsu **B84**, Res. Inst. Math. Sci. (RIMS), Kyoto (2021), 23–192; available at the following URL: `https://www.kurims.kyoto-u.ac.jp/~motizuki/Alien%20Copies,%20Gaussians,%20and%20Inter-universal%20Teichmuller%20Theory.pdf`

[EssLgc] S. Mochizuki, *On the essential logical structure of inter-universal Teich-müller theory in terms of logical AND "$\wedge$"/logical OR "$\vee$" relations: Report on the occasion of the publication of the four main papers on inter-universal Teichmüller theory*, RIMS Preprint **1968** (November 2022); updated version available at the following URL: `https://www.kurims.kyoto-u.ac.jp/~motizuki/Essential%20Logical%20Structure%20of%20Inter-universal%20Teichmuller%20Theory.pdf`

[RNSPM] S. Mochizuki, S. Tsujimura, *Resolution of Nonsingularities, Point-theoreticity, and Metric-admissibility for p-adic Hyperbolic Curves*, RIMS Preprint **1974** (June 2023).

[GSCsp] Y. Hoshi, S. Mochizuki, *Arithmetic cuspidalization of Galois sections of hyperbolic curves*, manuscript in preparation.

[AnPf] Y. Hoshi, S. Mochizuki, S. Tsujimura, G. Yamashita, *Anabelian geometry over complete discrete valuation rings with perfect residue fields*, manuscript in preparation.