KOLMOGOROV–SMIRNOV STATISTICS AND THE ANALYTIC PROPERTIES OF DIRICHLET SERIES ASSOCIATED TO ELLIPTIC CURVES

A Dissertation

Presented to the Faculty of the Graduate School

of Cornell University

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

by

Daniel Miller

May 2017

KOLMOGOROV–SMIRNOV STATISTICS AND THE ANALYTIC PROPERTIES OF DIRICHLET SERIES ASSOCIATED TO ELLIPTIC CURVES

Daniel Miller, Ph.D.
Cornell University 2017

Abstract here.

BIOGRAPHICAL SKETCH

Brief biographical sketch.

Dedication here.

ACKNOWLEDGEMENTS

For starters, I'd like to thank my parents Jay and Cindy for noticing and fostering my mathematical interests early on, and for being loving and supportive the whole way through. I'd also like to thank my undergraduate thesis advisor, Griffith Elder, without whose encouragement and inspiration I'd probably never have considered a career in math.

Thanks to my graduate student friends Sasha Patotski and Balázs Elek for sharing my early love of algebraic geometry, for laughing with me at the absurdities of academic life, and listening to my ramblings about number theory long after they'd stopped being interesting.

I owe a big debt of gratitude to the mathematics department at Cornell—so many professors were generous with their time and ideas. I especially appreciate Birgit Speh, Yuri Berest, David Zywina, Farbod Shokrieh, and John Hubbard for letting me bounce ideas off them, helping me add rigor to half-baked ideas, and pointing me in new and exciting directions.

I am especially thankful to my advisor Ravi. He kindled my first love for number theory, and stayed supportive as my research bounced all over the place, and helped focus and ground my thesis when I needed concrete results.

Lastly, I thank my loving wife Ivy for being there for me through the highs and the lows—both when I (prematurely) thought my thesis was complete, and when I thought my results were completely in shambles. I couldn't have done it without her.

TABLE OF CONTENTS

1 Introduction **1**

2 Discrepancy **2**
- 2.1 Definitions and first results . . . 2
- 2.2 The Koksma–Hlawka inequality . . . 2
- 2.3 Comparing sequences . . . 2
- 2.4 Combining sequences . . . 2

3 Strange Dirichlet series **3**
- 3.1 Definitions . . . 3
- 3.2 Relation to automorphic and motivic L-functions . . . 3
- 3.3 The Riemann Hypothesis . . . 3
- 3.4 Discrepancy of sequences and the Riemann Hypothesis . . . 3

4 Irrationality exponents **4**

5 Deformation theory **5**
- 5.1 Category of test objects . . . 5
- 5.2 Quotients in the flat topology . . . 6
- 5.3 Groupoids and quotient stacks . . . 8
- 5.4 Deformations of group representations . . . 8
- 5.5 Tangent spaces and obstruction theory . . . 9

6 Constructing Galois representations **11**

7 First counterexample **12**

8 Second counterexample **13**

9 Computational evidence for the Akiyama–Tanigawa conjecture **14**

10 Concluding remarks and future directions **15**

CHAPTER 1
INTRODUCTION

Let's start with something basic, an elliptic curve $E_{/\mathbf{Q}}$. For any prime l, we have the Tate module of E, written $\mathrm{T}_l E$. This is a rank-2 $\mathbf{Z}_l$-module with continuous $G_{\mathbf{Q}}$-action, so it induces a continuous representation

$$\rho_{E,l} \colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l).$$

It is known (citation?) that the quantities $a_p(E) = \operatorname{tr} \rho_l(\mathrm{fr}_p)$ lie in $\mathbf{Z}$ and satisfy the Hasse bound

$$|a_p(E)| < 2\sqrt{p}.$$

Thus we can define, for each prime p, the corresponding Satake parameter for E.

$$\theta_p(E) = \cos^{-1}\left(\frac{a_p(E)}{2\sqrt{p}}\right) \in [0, \pi).$$

The Satake parameters are packaged into an L-function as follows:

$$L(E, s) = \prod_p \frac{1}{(1 - e^{i\theta_p(E)} p^{-s})(1 - e^{-i\theta_p(E)} p^{-s})}.$$

Theorem: analytic continuation of $L(E, s)$ past $\Re s = 1$ is equivalent to the Sato–Tate conjecture, namely that the $\theta_p(E)$ are equidistributed.

Rephrase equidistribution. (Chebotarev, strong RH).

So S–T is equivalent to discrepancy being $o(N)$.

Riemann Hypothesis is implied by A–T.

Does converse hold?

No! We'll construct two classes of counterexamples.

And also provide computational evidence for the A–T conjecture (for elliptic curves and also generic abelian 2-folds).

CHAPTER 2
DISCREPANCY

2.1 Definitions and first results

regular discrepancy
star discrepancy
Euclidean space vs. torus

2.2 The Koksma–Hlawka inequality

d

2.3 Comparing sequences

If $\{x_n\} \subset [0, \pi/2)$ has some discrepancy with respect to some measure, then the "flipped" sequence $\{\pi/2 - x_n\}$ has the same discrepancy with respect to the "flipped" measure.

2.4 Combining sequences

If $\{x_n\}$ and $\{y_n\}$ are sequences supported on $[0, \pi/2)$ and $[\pi/2, \pi)$ respectively, and both are equidistributed with respect to measures supported on their respective intervals, then the "interleaved" sequence $(x_1, y_1, x_2, y_2, \dots)$ also has equidistribution (with respect to the combined measure) and discrepancy which decays no faster than the slower of the two.

CHAPTER 3
STRANGE DIRICHLET SERIES

3.1 Definitions

strange Dirichlet series for a series of complex numbers
...for a function and a sequence in the domain space

3.2 Relation to automorphic and motivic L-functions

3.3 The Riemann Hypothesis

3.4 Discrepancy of sequences and the Riemann Hypothesis

CHAPTER 4

IRRATIONALITY EXPONENTS

CHAPTER 5
DEFORMATION THEORY

5.1 Category of test objects

The following is an exposition and explication of the theory outlined in [SGA 3_1, $\mathrm{VII_B}$, §0–1]. In particular, we will heavily use the notions of a pseudocompact ring, pseudocompact modules, etc. Let Λ be a pseudocompact ring. Write C_Λ for the opposite of the category of Λ-algebras which have finite length as Λ-modules. Given such a Λ-algebra A, write $X = \mathrm{Spf}(A)$ for the corresponding object of C_Λ, and we put $A = \mathscr{O}(X)$.

Lemma 5.1.1. *Let Λ be a pseudocompact ring, C_Λ as above. Then C_Λ is closed under finite limits and colimits.*

Lemma 5.1.2. *Let Λ be a pseudocompact local ring. Then Λ is henselian, in any of the following senses:*

1. *d*

Proof. [EGA 4_4, 18.5.?] □

Following Grothendieck, if $\mathcal{C}$ is an arbitrary category, we write $\widehat{\mathcal{C}} = \hom(\mathcal{C}^\circ, \mathsf{Set})$ for the category of contravariant functors $\mathcal{C} \to \mathsf{Set}$. We regard $\mathcal{C}$ as a full subcategory of $\widehat{\mathcal{C}}$ via the Yoneda embedding, so for $X, Y \in \mathcal{C}$, we write $X(Y) = \hom_{\mathcal{C}}(Y, X)$. With this notation, the Yoneda Lemma states that $\hom_{\widehat{\mathcal{C}}}(X, P) = P(X)$ for all $X \in \mathcal{C}$.

Lemma 5.1.3. *Let $\mathcal{X} \in \widehat{\mathsf{C}_\Lambda}$. Then $\mathcal{X}$ is left exact if and only if there exists a filtered system $\{X_i\}_{i\in I}$ in $\mathcal{C}_\Lambda$ together with a natural isomorphism $\mathcal{X}(\cdot) \simeq \varinjlim X_i(\cdot)$. Write $\mathsf{Ind}(\mathsf{C}_\Lambda)$ for the category of such functors. Then $\mathsf{Ind}(\mathsf{C}_\Lambda)$ is closed under colimits, and the Yoneda embedding $\mathsf{C}_\Lambda \hookrightarrow \mathsf{Ind}(\mathsf{C}_\Lambda)$ preserves filtered colimits.*

Proof. This follows from the results of [KS06, 6.1]. □

If R is a pseudocompact Λ-algebra, write $\mathrm{Spf}(R)$ for the object of $\widehat{\mathsf{C}_\Lambda}$ defined by $\mathrm{Spf}(R)(A) = \hom_{\mathrm{cts}/\Lambda}(R, A)$, the set of continuous Λ-algebra homomorphisms.

Lemma 5.1.4. *The funtor* Spf *induces an (anti-)equivalence between the category of pseudocompact Λ-algebras and $\mathsf{Ind}(\mathsf{C}_\Lambda)$.*

Proof. This is [SGA 3_1, $\mathrm{VII_B}$ 0.4.2 Prop.]. □

So $\mathsf{Ind}(\mathsf{C}_\Lambda)$ is the category of pro-representable functors on finite length Λ-algebras. *Warning*: in many papers, for example the foundational [Maz97], one reserves the term *pro-representable* for functors of the form $\mathrm{Spf}(R)$, where R is *noetherian*. We do not make this restriction.

Lemma 5.1.5. *The category $\mathsf{Ind}(\mathsf{C}_\Lambda)$ is an exponential ideal in $\widehat{\mathsf{C}_\Lambda}$.*

Proof. By this we mean the following. Let $\mathcal{X} \in \mathsf{Ind}(\mathsf{C}_\Lambda)$, $P \in \widehat{\mathsf{C}_\Lambda}$. Then the functor $\mathcal{X}^P$ defined by

$$\mathcal{X}^P(S) = \hom_{\widehat{\mathsf{C}_\Lambda}_{/S}}(P_{/S}, \mathcal{X}_{/S})$$

is also in $\mathsf{Ind}(\mathsf{C}_\Lambda)$. Given the characterization of $\mathsf{Ind}(\mathsf{C}_\Lambda)$ as left exact functors, this is easy to prove, see e.g. [Joh02, 4.2.3]. □

If $\mathcal{C}$ is a category, we write $\mathsf{Gp}(\mathcal{C})$ for the category of group objects in $\mathcal{C}$.

Corollary 5.1.6. *Let $\Gamma \in \mathsf{Gp}(\widehat{\mathsf{C}_\Lambda})$ and $\mathcal{G} \in \mathsf{Gp}(\mathsf{Ind}(\mathsf{C}_\Lambda))$, then the functor $[\Gamma, \mathcal{G}]$ defined by*

$$[\Gamma, \mathcal{G}](S) = \hom_{\mathsf{Gp}/S}(\Gamma_{/S}, \mathcal{G}_{/S})$$

is in $\mathsf{Ind}(\mathsf{C}_\Lambda)$. In particular, if Γ is a profinite group, then the functor

$$[\Gamma, \mathcal{G}](S) = \hom_{\mathrm{cts}/\,\mathsf{Gp}}(\Gamma, \mathcal{G}(S))$$

is in $\mathsf{Ind}(\mathsf{C}_\Lambda)$.

Proof. The first claim follows easily from 5.1.5. Just note that $[\Gamma, \mathcal{G}]$ is the equalizer:

$$[\Gamma, \mathcal{G}] \longrightarrow \mathcal{G}^\Gamma \underset{m_{\mathcal{G}*}}{\overset{m_\Gamma^*}{\rightrightarrows}} \mathcal{G}^{\Gamma\times\Gamma},$$

that is, those $f \colon \Gamma \to \mathcal{G}$ such that $f \circ m_\Gamma = m_{\mathcal{G}} \circ (f \times f)$. The latter claim is just a special case. ☐

5.2 Quotients in the flat topology

If Λ is a pseudocompact ring, the category $\mathsf{Ind}(\mathsf{C}_\Lambda)$ has nice "geometric" properties. However, for operations like taking quotients, we will embed it into the larger category $\mathsf{Sh}_{\mathrm{fl}}(\mathsf{C}_\Lambda)$ of flat sheaves. We call a collection $\{U_i \to X\}$ of morphisms in C_Λ a *flat cover* if each ring map $\mathscr{O}(X) \to \mathscr{O}(U_i)$ is flat, and moreover $\mathscr{O}(X) \to \prod \mathscr{O}(U_i)$ is faithfully flat. By [SGA 3_1, IV 6.3.1], this is a subcanonical Grothendieck topology on C_Λ. We call it the *flat topology*, even though finite presentation comes for free because all the rings are finite length.

Lemma 5.2.1. *Let $\mathsf{Sh}_{\mathrm{fl}}(\mathsf{C}_\Lambda)$ be the category of sheaves (of sets) on C_Λ with respect to the flat topology. Then a presheaf $P \in \widehat{\mathsf{C}_\Lambda}$ lies in $\mathsf{Sh}_{\mathrm{fl}}(\mathsf{C}_\Lambda)$ if and only if $P(\coprod U_i) = \prod P(U_i)$ and moreover, whenever $U \to X$ is a flat cover where $\mathscr{O}(U)$ and $\mathscr{O}(X)$ are local rings, the sequence*

$$P(X) \longrightarrow P(U) \rightrightarrows P(U \times_X U).$$

is exact. Moreover, $\mathsf{Ind}(\mathsf{C}_\Lambda) \subset \mathsf{Sh}_{\mathrm{fl}}(\mathsf{C}_\Lambda)$.

Proof. The first claim is the content of [SGA 3_1, IV 6.3.1(ii)]. For the second, note that any $\mathcal{X} \in \mathsf{Ind}(\mathsf{C}_\Lambda)$ will, by 5.1.3, convert (arbitrary) colimits into limits. Thus $\mathcal{X}(\coprod U_i) = \prod \mathcal{X}(U_i)$. If $U \to X$ is a flat cover, then by (loc. cit.), $U \times_X U \rightrightarrows U \to X$ is a coequalizer diagram in C_Λ, hence $\mathcal{X}(X) \to \mathcal{X}(U) \rightrightarrows \mathcal{X}(U \times_X U)$ is an equalizer. ☐

Our main reason for introducing the category $\mathsf{Sh}_{\mathrm{fl}}(\mathsf{C}_\Lambda)$ is that, as a (Grothendieck) topos, it is closed under arbitrary colimits. Recall that in an *equivalence relation* in $\widehat{\mathsf{C}_\Lambda}$ is a morphism $R \to X \times X$ such that, for all S, the map $R(S) \to X(S) \times X(S)$ is an injection whose image is an equivalence relation on $X(S)$. We define the quotient X/R to be the coequalizer

$$R \rightrightarrows X \longrightarrow X/R.$$

By Giraud's Theorem [MLM94, App.], for any $S \in \mathsf{C}_\Lambda$, the natural map $X(S)/R(S) \to (X/R)(S)$ is injective. It will not be surjective in general.

We let $\mathsf{Sh}_{\mathrm{fl}}(\mathsf{C}_\Lambda)$ inherit definitions from C_Λ as follows. If P is a property of maps in C_Λ (for example, "flat," or "smooth,") and $f \colon X \to Y$ is a morphism in $\mathsf{Sh}_{\mathrm{fl}}(\mathsf{C}_\Lambda)$, we say that f has P if for all $S \in \mathsf{C}_\Lambda$ and $y \in Y(S)$, the pullback $X_S = X \times_Y S$ lies in C_Λ, and the pullback map $X_S \to S$ has property P. For example, if $X = \mathrm{Spf}(R')$ and $Y = \mathrm{Spf}(R)$, then $X \to Y$ has property P if and only if for all finite length A and continuous Λ-algebra maps $R \to A$, the induced map $A \to R' \otimes_R A$ has P.

Theorem 5.2.2. *Let $\mathcal{R} \to \mathcal{X} \times \mathcal{X}$ be an equivalence relation in $\mathsf{Ind}(\mathsf{C}_\Lambda)$ such that one of the maps $\mathcal{R} \to \mathcal{X}$ is flat. Then the quotient $\mathcal{X}/\mathcal{R}$ lies in $\mathsf{Ind}(\mathsf{C}_\Lambda)$, and $\mathcal{X} \to \mathcal{X}/\mathcal{R}$ is a flat cover.*

Proof. This is [SGA 3_1, $\mathrm{VII_B}$ 1.4]. □

By [Mat89, 29.7], if k is a field and R is a complete regular local k-algebra, then $R \simeq k[\![t_1, \dots, t_n]\!]$. In particular, R admits an augmentation $\epsilon\colon R \to k$. There is a general analogue of this result, but first we need a definition.

Definition 5.2.3. *A map $f\colon \mathcal{X} \to \mathcal{Y}$ in $\mathsf{Ind}(\mathsf{C}_\Lambda)$ is a* residual isomorphism *if for all $S = \mathrm{Spf}(k) \in \mathsf{C}_\Lambda$ where k is a field, the map $f\colon \mathcal{X}(S) \to \mathcal{Y}(S)$ is a bijection.*

Lemma 5.2.4. *Let $f\colon \mathcal{X} \to \mathcal{Y}$ be a smooth map in $\mathsf{Ind}(\mathsf{C}_\Lambda)$ that is a residual isomorphism. Then f admits a section.*

Proof. By [SGA 3_1, $\mathrm{VII_B}$ 0.1.1], it suffices to prove the result when $\mathcal{X} = \mathrm{Spf}(R')$, $\mathcal{Y} = \mathrm{Spf}(R)$, for local Λ-algebras $R \to R'$ with the same residue field. Let $k = R/\mathfrak{m}_R \xrightarrow{\sim} R'/\mathfrak{m}_{R'}$ be their common residue field. From the diagram

$$\begin{tikzcd} R' \arrow[r, dotted] \arrow[dr, two heads] & R \arrow[d, two heads] \\ R \arrow[u] \arrow[r, two heads] \arrow[ur, equal] & k, \end{tikzcd}$$

the definition of (formal) smoothness, and a limiting argument involving the finite length quotients $R/\mathfrak{a}$, we obtain the result. □

Corollary 5.2.5. *Let $\mathcal{R} \to \mathcal{X} \times \mathcal{X}$ be an equivalence relation satisfying the hypotheses of 5.2.2. Suppose further that*

1. *One of the maps $\mathcal{R} \to \mathcal{X}$ is smooth, and*
2. *The projection $\mathcal{X} \to \mathcal{X}/\mathcal{R}$ is a residual isomorphism.*

Then $\mathcal{X} \to \mathcal{X}/\mathcal{R}$ admits a section, so $\mathcal{X}(S)/\mathcal{R}(S) \xrightarrow{\sim} (\mathcal{X}/\mathcal{R})(S)$ for all $S \in \mathsf{C}_\Lambda$.

Proof. By 5.2.4, it suffices to prove that $\mathcal{X} \to \mathcal{X}/\mathcal{R}$ is smooth. By [EGA 4_4, 17.7.3(ii)], smoothness can be detected after flat descent. So base-change with respect to the projection $\mathcal{X} \to \mathcal{X}/\mathcal{R}$. In the following commutative diagram

$$\begin{tikzcd} \mathcal{R} \arrow[dr, equal] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\ & \mathcal{X} \times_{\mathcal{X}/\mathcal{R}} \mathcal{X} \arrow[r] \arrow[d] & \mathcal{X} \arrow[d] \\ & \mathcal{X} \arrow[r] & \mathcal{X}/\mathcal{R} \end{tikzcd}$$

we can ensure the smoothness of $\mathcal{R} \to \mathcal{X}$ by our hypotheses. Since $\mathcal{X} \to \mathcal{X}/\mathcal{R}$ is smooth after flat base-change, the original map is smooth. □

Example 5.2.6. The hypothesis on residue fields in 5.2.5 is necessary. To see this, let $\Lambda = k$ be a field, $k \hookrightarrow K$ a finite Galois extension with Galois group G. Then $G \times \mathrm{Spf}(K) \rightrightarrows \mathrm{Spf}(K)$ has quotient $\mathrm{Spf}(k)$, but the map $\mathrm{Spf}(K)(S) \to \mathrm{Spf}(k)(S)$ is *not* surjective for all $S \in \mathsf{C}_k$, e.g. it is not for $S = \mathrm{Spf}(k)$.

Example 5.2.7. The hypothesis of smoothness in 5.2.5 is necessary. To see this, let k be a field of characteristic $p > 0$. Then the formal additive group $\widehat{\mathbf{G}}_{\mathrm{a}} = \mathrm{Spf}(k[\![t]\!])$ has a subgroup $\boldsymbol{\alpha}_p$ defined by

$$\boldsymbol{\alpha}_p(S) = \{s \in \mathscr{O}(S) \colon s^p = 0\}.$$

The quotient $\widehat{\mathbf{G}}_{\mathrm{a}}/\boldsymbol{\alpha}_p$ has as affine coordinate ring $k[\![t^p]\!]$. In particular, the following sequence is exact in the flat topology:

$$0 \longrightarrow \boldsymbol{\alpha}_p \longrightarrow \widehat{\mathbf{G}}_{\mathrm{a}} \xrightarrow{(\cdot)^p} \widehat{\mathbf{G}}_{\mathrm{a}} \longrightarrow 0.$$

It follows that $\boldsymbol{\alpha}_p \times \widehat{\mathbf{G}}_{\mathrm{a}} \rightrightarrows \widehat{\mathbf{G}}_{\mathrm{a}} \xrightarrow{(\cdot)^p} \widehat{\mathbf{G}}_{\mathrm{a}}$ is a coequalizer in $\mathsf{Sh}_{\mathrm{fl}}(\mathsf{C}_k)$ satisfying all the hypothese of 5.2.5 except smoothness. And indeed, as one sees by letting $S = \mathrm{Spf}(A)$ for any non-perfect k-algebra A, the map $(\cdot)^p \colon \widehat{\mathbf{G}}_{\mathrm{a}}(S) \to \widehat{\mathbf{G}}_{\mathrm{a}}(S)$ is *not* surjective for all S.

5.3 Groupoids and quotient stacks

Lemma 5.3.1. *Let $\mathcal{G} \in \mathsf{Ind}(\mathsf{C}_\Lambda)$ be a smooth connected group. Then every $\mathcal{G}$-torsor is trivial.*

Proof. Let $\mathcal{P} \to \mathcal{B}$ be a $\mathcal{G}$-torsor in $\mathsf{Ind}(\mathsf{C}_\Lambda)$. That is, $\mathcal{P}$ has an action of $\mathcal{G}_{\mathcal{S}}$ for which $\mathcal{P} \times_{\mathcal{B}} \mathcal{P} \simeq \mathcal{G} \times \mathcal{P}$ as $\mathcal{G}$-spaces. [. . . not done. . .] $\square$

Theorem 5.3.2. *Let $\mathcal{G}$ be a smooth connected group in $\mathsf{Ind}(\mathsf{C}_\Lambda)$, and $\mathcal{X} \in \mathsf{Ind}(\mathsf{C}_\Lambda)$ a $\mathcal{G}$-object. Then the quotient stack $[\mathcal{X}/\mathcal{G}](S)$ has as objects $\mathcal{X}(S)/\mathcal{G}(S)$, but with extra automorphisms?*

Proof. Use triviality of torsors. $\square$

5.4 Deformations of group representations

Let $\Gamma \in \mathsf{Gp}(\widehat{\mathsf{C}_\Lambda})$ and $\mathcal{G} \in \mathsf{Ind}(\mathsf{C}_\Lambda)$. By 5.1.6, the functor

$$\mathrm{Rep}^{\square}(\Gamma, \mathcal{G})(S) = \hom_{\mathsf{Gp}/S}(\Gamma_S, \mathcal{G}_S)$$

is in $\mathsf{Ind}(\mathsf{C}_\Lambda)$. We would like to define an ind-scheme $\mathrm{Rep}(\Gamma, \mathcal{G})$ as "$\mathrm{Rep}^{\square}(\Gamma, \mathcal{G})$ modulo conjugation," but this requires some care. The conjugation action of $\mathcal{G}$ on $\mathrm{Rep}^{\square}(\Gamma, \mathcal{G})$ will have fixed points, so the quotient will be badly behaved. We loosely follow [Til96].

Assume Λ is local, with maximal ideal $\mathfrak{m}$ and residue field $\mathbf{k}$. Fix $\bar\rho \in \mathrm{Rep}^{\square}(\Gamma, \mathcal{G})(\mathbf{k})$, i.e. a residual representation $\bar\rho \colon \Gamma \to \mathcal{G}(\mathbf{k})$. Let $\mathrm{Rep}^{\square}(\Gamma, \mathcal{G})_{\bar\rho}$ be the connected component of $\bar\rho$ in $\mathrm{Rep}^{\square}(\Gamma, \mathcal{G})$. Assume that $\mathcal{G}$ and $\mathrm{Z}(\mathcal{G})$ are smooth; then the quotient $\mathcal{G}^{\mathrm{ad}} = \mathcal{G}/\mathrm{Z}(\mathcal{G})$ is also smooth. Let $\mathcal{G}^{\mathrm{ad},\circ}$ be the connected component of 1 in $\mathcal{G}^{\mathrm{ad}}$.

Theorem 5.4.1. *Suppose $(\Lambda, \mathfrak{m}, \mathbf{k})$ is local. If $\mathcal{X}, \mathcal{Y} \in \mathsf{Ind}(\mathsf{C}_\Lambda)$ are connected and $\mathcal{X}(\mathbf{k}) \neq \varnothing$, then $\mathcal{X} \times_\Lambda \mathcal{Y}$ is connected.*

Proof. We are reduced to proving the following result from commutative algebra: if R, S are local pro-artinian Λ-algebras and R has residue field $\mathbf{k}$, then $R \widehat{\otimes}_\Lambda S$ is local. Since $R \widehat{\otimes}_\Lambda S = \varprojlim (R/\mathfrak{r}) \otimes_\Lambda (S/\mathfrak{s})$, $\mathfrak{r}$ (resp. $\mathfrak{s}$) ranges over all open ideals in R (resp. S), we may assume that both R and S are artinian. The rings R and S are henselian, so $R \otimes S$ is local if and only if $(R/\mathfrak{m}_R) \otimes (S/\mathfrak{m}_S) = S/\mathfrak{m}_S$ is local, which it is. $\square$

We conclude that the action of $\mathcal{G}^{\mathrm{ad},\circ}$ on $\mathrm{Rep}^{\square}(\Gamma, \mathcal{G})$ preserves $\mathrm{Rep}^{\square}(\Gamma, \mathcal{G})_{\bar\rho}$. Thus we may put

$$\mathrm{Rep}(\Gamma, \mathcal{G})_{\bar\rho} = [\mathrm{Rep}^{\square}(\Gamma, \mathcal{G})_{\bar\rho}/\mathcal{G}^{\mathrm{ad},\circ}].$$

If $\mathcal{G}^{\mathrm{ad},\circ}$ acts faithfully on $\mathrm{Rep}^{\square}(\Gamma, \mathcal{G})_{\bar\rho}$, then we recover the classical notion of the deformation functor.

Theorem 5.4.2. *Let Γ be a profinite group, $\bar\rho\colon \Gamma \to \mathcal{G}(\mathbf{k})$ a representation with $\mathrm{H}^0(\Gamma, \mathrm{Ad}\,\bar\rho) = 0$. Then $\mathrm{Rep}(\Gamma, \mathcal{G})_{\bar\rho}$ exists and is what you expect.*

Proof. Need assumptions on $\mathrm{Z}(\mathcal{G})$, $\mathcal{G}$ should be smooth.

Need $\mathrm{Z}(\mathcal{G}) = \ker(\mathcal{G} \to \mathrm{GL}(\mathfrak{g}))$ in connected case. This should use $\mathfrak{g} = \mathrm{Lie}(\mathrm{Aut}\,\mathcal{G})$, via deviations in [SGA 3_1]. □

[. . . local conditions]

5.5 Tangent spaces and obstruction theory

For $S_0 \in \mathsf{C}_\Lambda$, let Ex_{S_0} be the category of square-zero thickenings of S_0. An object of Ex_{S_0} is a closed embedding $S_0 \hookrightarrow S$ whose ideal of definition has square zero. Should be "exponential exact sequence"

$$0 \longrightarrow \mathfrak{g}(I) \longrightarrow \mathcal{G}(S) \longrightarrow \mathcal{G}(S_0) \longrightarrow 1$$

This gives us a class $\exp \in \mathrm{H}^2(\mathcal{G}(S_0), \mathfrak{g}(I))$. For $\rho_0\colon \Gamma \to \mathcal{G}(S_0)$, the obstruction class is $o(\rho_0, I) = \rho_0^*(\exp) \in \mathrm{H}^2(\Gamma, \mathfrak{g}(I))$. It's easy to check that $o(\rho_0, I) = 0$ if and only if ρ_0 lifts to ρ. So obstruction theory naturally for $\mathrm{Rep}^\square(\Gamma, \mathcal{G})$.

[Use [Wei94, 6.6.4]. Given setting as above, $\rho_0^*(\exp)$ is the pullback by ρ_0:

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{g}(I) \arrow[r] \arrow[d, equal] & \mathcal{G}(S) \times_{\mathcal{G}(S_0)} \Gamma \arrow[r] \arrow[d] & \Gamma \arrow[r] \arrow[d, "\rho_0"] & 1 \\
0 \arrow[r] & \mathfrak{g}(I) \arrow[r] & \mathcal{G}(S) \arrow[r] & \mathcal{G}(S_0) \arrow[r] & 1
\end{tikzcd}$$

Computing explicitly, we see the result.]

Proposition 5.5.1. *Let $f\colon G \to H$ be a morphism of profinite groups. Suppose M is a discrete H-module and $c \in \mathrm{H}^2(H, M)$ corresponds to the extension*

$$0 \longrightarrow M \longrightarrow \widetilde{H} \longrightarrow H \longrightarrow 1.$$

Then $f^*c = 0$ in $\mathrm{H}^2(G, M)$ if and only if there is a map $\widetilde{f}\colon G \to \widetilde{H}$ making the following diagram commute:

$$\begin{tikzcd}
& \widetilde{H} \arrow[dd] \\
G \arrow[ur, "\widetilde{f}"] \arrow[dr, "f"'] & \\
& H.
\end{tikzcd}$$

Proof. By [Wei94, 6.6.4], the class f^*c corresponds to the pullback diagram:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, equal] & G \times_H \widetilde{H} \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, "f"] & 1 \\
0 \arrow[r] & M \arrow[r] & \widetilde{H} \arrow[r] & H \arrow[r] & 1.
\end{tikzcd}$$

Writing explicitly what it means for $G \times_H \widetilde{H} \to G$ to split yields the result. □

Let $\mathcal{X} \in \mathsf{Ind}(\mathsf{C}_{/\Lambda})$ be smooth, and $\mathrm{L}_{\mathcal{X}/\Lambda} \simeq \Omega^1_{\mathcal{X}/\Lambda}[0]$ be its cotangent complex. Fix $x_0 \in \mathcal{X}(S_0)$. From the chain $S_0 \xrightarrow{x_0} \mathcal{X} \to \mathrm{Spf}(\Lambda)$, we get a distinguished triangle [Ill71, II 2.1.5.6]

$$x_0^*\mathrm{L}_{\mathcal{X}/\Lambda} \longrightarrow \mathrm{L}_{S_0/\Lambda} \longrightarrow \mathrm{L}_{S_0/\mathcal{X}} \longrightarrow .$$

If I is a coherent sheaf on S_0, we get a long exact sequence:

$$\mathrm{Ext}^0(\mathrm{L}_{S_0/\Lambda}, M) \longrightarrow \mathrm{Ext}^0(x_0^*\mathrm{L}_{\mathcal{X}/\Lambda}, M) \longrightarrow \mathrm{Ext}^1(\mathrm{L}_{S_0/\mathcal{X}}, M) \longrightarrow \mathrm{Ext}^1(\mathrm{L}_{S_0/\Lambda}, M) \longrightarrow \mathrm{Ext}^1(x_0^*\mathrm{L}_{\mathcal{X}/\Lambda}, M)$$

If $\mathcal{X}_{/\Lambda}$ is smooth, then $\mathrm{Ext}^1(x_0^*\mathrm{L}_{\mathcal{X}/\Lambda}, M) = 0$ and $\mathrm{L}_{\mathcal{X}/\Lambda} = \Omega^1_{\mathcal{X}/\Lambda}$. This gives us an exact sequence

$$\mathrm{Ext}^0(\mathrm{L}_{S_0/\Lambda}, M) \longrightarrow \hom(\Omega^1_{\mathcal{X}/\Lambda}, M) \longrightarrow \mathrm{Ext}^1(\mathrm{L}_{S_0/\mathcal{X}}, M) \longrightarrow \mathrm{Ext}^1(\mathrm{L}_{S_0/\Lambda}, M) \longrightarrow 0.$$

The result [Ill71, III 2.1.7] tells us that the choice of $S \in \mathsf{Ex}_{S_0}(M)$ gives us an element of $\mathrm{Ext}^1(\mathrm{L}_{S_0/\Lambda}, M)$. Its fiber admits an action of $\hom(\Omega^1_{\mathcal{X}/\Lambda}, M)$. The only thing remaining is: we need $\mathrm{Ext}^0(\mathrm{L}_{S_0/\Lambda}, M) = 0$, which doesn't hold in complete generality.

CHAPTER 6

CONSTRUCTING GALOIS REPRESENTATIONS

CHAPTER 7
FIRST COUNTEREXAMPLE

CHAPTER 8
SECOND COUNTEREXAMPLE

CHAPTER 9

COMPUTATIONAL EVIDENCE FOR THE AKIYAMA–TANIGAWA CONJECTURE

CHAPTER 10
CONCLUDING REMARKS AND FUTURE DIRECTIONS

BIBLIOGRAPHY

[EGA 4_4] Alexandre Grothendieck. *Éléments de gómétrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV*. 32. 1967.

[SGA 3_1] Alexandre Grothendieck and Michel Demazure, eds. *Schémas en groupes (SGA 3). Tome I. Propriétés générales des schémas en groupes*. Vol. 151. Lecture Notes in Mathematics. Springer-Verlag, 1970.

[Ill71] Luc Illusie. *Complexe cotangent et déformations. I*. Vol. 239. Lecture Notes in Mathematics. Springer-Verlag, 1971.

[Joh02] Peter Johnstone. *Sketches of an elephant: a topos theory compendium*. Vol. 44, 45. Oxford Logic Guides. Oxford University Press, 2002.

[KS06] Massaki Kashiwara and Pierre Schapira. *Categories and sheaves*. Vol. 332. Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, 2006.

[MLM94] Saunders Mac Lane and Ieke Moerdijk. *Sheaves in geometry and logic*. Second. Universitext. A first introduction to topos theory. Springer-Verlag, 1994.

[Mat89] Hideyuki Matsumura. *Commutative ring theory*. Second. Vol. 8. Cambridge Studies in Advanced Mathematics. Translated from the Japanese by M. Reid. Cambridge University Press, 1989.

[Maz97] Barry Mazur. "An introduction to the deformation theory of Galois representations". In: *Modular forms and Fermat's last theorem (Bostom, MA, 1995)*. New York: Springer, 1997, pp. 243–311.

[Til96] Jacques Tilouine. *Deformations of Galois representations and Hecke algebras*. Mehta Research Institute of Mathematics, 1996.

[Wei94] Charles Weibel. *An introduction to homological algebra*. Vol. 38. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1994.