数理解析研究所講究録 第2120巻 2019年 72-152

On $(\infty \times p)$-adic uniformization of curves mod p with assigned many rational points

Yasutaka Ihara
RIMS, Kyoto University (P.E.)

I would like to express my deep gratitude to the organizers of this conference which itself was a great pleasure for me in all sense, and to the participants, some from far abroad, including especially the speakers. As a listener, I enjoyed all talks. Sometimes I felt insecure to have been "lifted up" higher than usual in the air, but each time the "plane" landed safely bringing me to some new fresh land.

The organizers have kindly invited me also to speak; I felt I was expected to give a brief account of some past work together with some remaining open problems. I accepted with pleasure, and asked if the talk could be divided into two shorter ones on separate days. I decided the subject, the title, and started reconsidering the open problems. They are related to the subject and the problems stated in the "Author's Notes (2008)" of [8]. Since the organizers generously agreed to divide the talk into two, I planned to use the first talk on a brief review and the second on "the lifting problem", one of the main open problems in *loc.cit,* which I believe to be still open. Then I started thinking "should I just propose it as an open problem, or ...? Isn't this so interesting!" Then some work, followed by repeated helpful discussions with A.Tamagawa for checking. Each talk expanded, and even more so this report.

The additions in this report are (i) details related to new or unpublished statements, (ii) brief memory of encounter with my real teachers, Professors G. Shimura, M. Kuga and I. Satake during 1958-63 while I was a student, and (iii) a few pages to remember and celebrate the discovery of supersingular elliptic curves and their moduli which took place about 80 years ago and to which the present work owes so deeply.

The main contents of this report are as follows. Among them the first four chapters are brief reviews which I thought necessary to understand the last two which hopefully contain something new.

(0) *Memories of my teachers*; Encounter with Professors G.Shimura, M. Kuga and I. Satake.

(Ch. I) *A student's viewpoint;* Encounter with the group $SL_2(Z[1/p])$; (∞ xp)-adic focusing; its advantage and disadvantage; encounter with supersingular moduli, Celebration of the (nearly) 80 years anniversary of discovery of supersingular elliptic curves, moduli, and their connection with the arithmetic of quaternion algebras (I-3).

(Ch. II) *Analogues of the Selberg ζ -function;* How the series of "congruence monodromy conjectures" arose naturally from the computation of an analogue of Selberg ζ -function for ($\infty \times \mathfrak{p}$)-adic lattices Γ generalizing $SL_2(Z[1/p])$, and how they had been verified. It relates each Γ (say, cocompact, torsion-free) with a pair ($\mathbf{X}$,$\mathfrak{S}$) of a curve $\mathbf{X}$ over $\mathbf{F}_{q^2}$ (q=N($\mathfrak{p}$)) and a set $\mathfrak{S}$ of $\mathbf{F}_{q^2}$ -rational points of $\mathbf{X}$ with cardinality (q-l)($g_{\mathbf{X}}$−1), in such a way that Γ = "π_1^{arith} ($\mathbf{X}$,$\mathfrak{S}$)".

(Ch.III) *Geometric objects inbetween Γ and ($\mathbf{X}$,$\mathfrak{S}$);* Groups Γ correspond functorially with systems of 3 complex curves (analogues of the Hecke correspondence T(p) desingularized); while the pairs ($\mathbf{X}$,$\mathfrak{S}$) correspond with systems of 3 curves over $\mathbb{F}_{q^2}$ (analogous to T(p) mod p). A "bridge" is what relates these two.

(Ch. IV) *Schwarzian operators and Frobenius-associated differentials;* Those algebraic differential equations on these systems of curves are discussed systematically, whose solutions on the complex curves side are d(g(τ)), g$\in$PGL$_2$(**C**): a parameter and τ : a variable on the Poincare upper half plane, while whose solutions on the p- side are cω (c: constants), where $\omega = \lim \omega_n$ is the differential associated with the lifting of Frobenius arising from a lifting of the system. The comparison theorem.

(Ch. V) *The dlog form of ω_n when $q=p=\pi$.* In this case, each ω_n is of the form dlog t_n. Formal results needed in Ch VI, followed by a concrete algebraic construction of these elements for the elliptic modular case using *only* the arithmetic Galois theory (non-compact "Galois group") of the field of modular functions of p-power levels. Elementary but pretty, like a construction in Euclidean geometry.

(Ch .VI) *The lifting problem.* Roughly speaking, this is to construct "T(p)" from the characteristic p side, step by step. The differential ω_n associated with a lifting of a Frobenius plays a crucial role, because one has local-global principle. After reviewing this and an old result on the first step lifting (to mod p^2), we proceed to attack the next step (to mod p^3) where two new phenomena appear. One is the appearance of a p-cyclic extension and the other is the difficulty in local description of this extension, arising from the fact that elements of the base field, the field of power series in 1-variable, have no canonical "names". We discuss our method and give an explicit answer Theorem VI-7.

(*References*) Reference A and B; the latter is for my own papers independently numbered.

Open problems, questions, conjectures (some vague, some explicit) are proposed in

II-4, III-3, IV-5(5), IV-7, V-3, VI-1, VI-4

[Memories of my Teachers]

(Undergraduate; 57-61 Spring) *Professors Goro Shimura* and *Michio Kuga*.

There were two separate Dept. of Math. in the University of Tokyo; one in the Faculty of General Educations (Komaba campus) and the other in the Faculty of Science (Hongo campus). The former was for the first two year undergraduate students whose faculty members' offices were in 第一研究室 (Daiichi Kenkyushitsu), an old building in row with, and looking like one of, the boys' dormitories. Along the corridor we could find such name plates of young faculty members as

志村五郎 (Goro Shimura) 谷山豊 (Yutaka Taniyama)

久賀道郎 (Michio Kuga) 岩堀長慶 (Nagayoshi Iwahori).

It was not an ivory tower, so when I had questions or was excited by small discoveries, I (after having gone around the dormitories with hesitations) went up the stairs to the corridor. I was very lucky to have had opportunities to see these young but leading mathematicians privately at an early stage of my mathematical life. (Shimura and Taniyama were well-known to the students already, and to everyone's great shock Taniyama suddenly passed away in November '58).

Kuga was also the teacher of my freshman calculus class, very enthusiastic and enlightening, and also personally I was encouraged by him so much that I felt like reborn. He suggested me to try to read such classics as Pontryagin, Weyl, Riemann, Hecke, etc., and to study Shimura-Taniyama theory (complex multiplication of abelian varieties and its applications to number theory). Very nourishing.

Shimura encouraged me in a different way. He was saying something like "you are good and bad" , but sometime later showed me the draft of his newest paper and even asked me to check details. This was another kind of great encouragement. When I was a 4th year undergraduate student, he kindly accepted to be my seminar(informal) adviser. Only Hongo teachers could become a formal adviser and Professor Iyanaga, whose seminar was said to be overcrowded, had generously agreed to be my formal adviser for this year.

For the seminar, Shimura suggested as textbook, first A.Weil's paper "Généralisation des fonctions abéliennes". Later I heard Kuga asking Shimura why he had chosen such a high level paper and Shimura answering that he wanted to see whether Ihara could give it an algebraic formulation!. "How could I ?", but I learnt something from this; sometimes even students can directly make basic innovations in this field of research, and they expect so much of us!. After this, instead of standard textbooks in classfield theory or foundational algebraic geometry (the students had to be able to read such textbooks by themselves), he chose de Rham's book on differential geometry, as a preparation to Weil's "variétés kaehlériennes" to which we did not reach within a year. Teachers in those days used to choose for their seminars those books that they wanted to read had they the spare time, and not those with which they were familiar. I understood this idea quite well. Before my graduation and going on to the graduate school, I was so shocked to hear that Shimura was leaving to Osaka University. "...Why?..." After about two years he moved permanently to Princeton University.

(Master's course; 61-63 Spring) *Professor Ichiro Satake.*

My adviser as graduate student was Professor Satake. I studied, in addition to Shimura's papers, some basics of arithmetic of algebraic groups, from Weil's "Adeles and algebraic groups" and three illuminating series of lectures by Satake on (i) quadratic forms, (ii) algebraic groups, and (iii) spherical functions. Also the famous paper of Selberg "Harmonic analysis and discontinuous groups...", Gelfand-Graev papers on unitary representations of SL(2) over p-adic fields (in a seminar held by Dr. A. Orihara), etc. But alas..., he also left Tokyo, for Chicago after summer 1962 . Before leaving, Satake gave a very inspiring lecture on "representation-theoretic interpretation of the Ramanujan conjecture". It was a point of departure for my work (Ch.I-1 below).

After he left, for the remaining few months of my Master's course, my formal adviser was Professor N.Iwahori. During this period, I worked for my Master's thesis and Satake encouraged me so warmly through airmail communications. Once, from Paris, he wrote back "here everything is *"fonctorisé"* ; now I met an interesting mathematics!", and gave me very helpful pieces of advice. (It was much later that I understood the significance of functorisations. I walked around the corridor in Tokyo but not on the pavements in Paris.)

During this period I also encountered Professor Mikio Sato, who had returned from IAS with his breakthrough towards the proof of the

Ramanujan conjecture based on a suggestion of Kuga, also in IAS about the same time. The combination of their ideas with old results of Deuring later turned out to be the subject of my PhD thesis, but this is another story.

It was a period of brain drain. Movement of the teachers from whom I was most influenced during this period in Tokyo area were, according to my memory and approximately(*) as follows.
(Hg=U.Tokyo Hongo; Kb=U.Tokyo Komaba; Os=Osaka U; Pr=Princeton U; IH=IHES, IA=IAS. Ch=U.Chicago; TE=Tokyo Educational U.)

Academic year (April-March)	58	59	60	61	62	63
Shimura	Kb	I H	Kb	Os	Os	Pr
Kuga	Kb	Kb	Kb	Kb/IA	IA	IA/...
Satake			IH/Hg	Hg	Hg/Ch	Ch
Iwahori	Kb	Hg	Hg/IA	IA	IA/Hg	Hg
M.Sato			TE/IA	IA	IA/TE	Os

Permanent Professors in number theory in Hongo were S. Iyanaga, Y.Kawada and M. Sugawara. Professor Tsuneo Tamagawa was an Associate Professor when I moved to Hongo in 59 but soon left for Yale.

—————————

(*) I asked the general manager's office of the Graduate School of Mathematical Sciences University of Tokyo (which grew out of two Departments of Mathematics mentioned above) for related official records. But they said they do not keep records of teachers of old Math. Departments, and added that they consider some records as secret because of "privacy". I still do not understand why.

I A student's viewpoint

I-1 I. Satake (1961). "A representation theoretic formulation of the Ramanujan Conjecture (R_jC_j)" (1)

[Adelic]

$$SL_2(\mathbb{Q}_A) = SL_2(\mathbb{R}) \times \prod_\ell{}' SL_2(\mathbb{Q}_\ell) \overset{\text{acts}}{\curvearrowright} L^2\left(SL_2(\mathbb{Q}_A)/SL_2(\mathbb{Q})\right)$$

$$\cup \text{ open}$$

$$\prod_\ell SL_2(\mathbb{Z}_\ell)$$

any irreducible "component"

$$\rho = \rho_\infty \otimes \prod_\ell \rho_\ell$$

$$\rho_\ell \in Repr(SL_2(\mathbb{Q}_\ell))$$

$(R_jC_j) \longleftrightarrow$ for each ρ,

$\rho_\infty \in$ holomorphic discrete series $\Rightarrow \rho_p$: "tempered" for all p

[$(\infty \times p)$-adic] I asked myself.. Then why not focus only on the relevant part:

$$(SL_2)_{\infty,p} := SL_2(\mathbb{R}) \times SL_2(\mathbb{Q}_p) \curvearrowright L^2\left((SL_2)_{\infty,p}/SL_2(\mathbb{Z}[\tfrac{1}{p}])\right) \quad ?$$

$$\rho = \rho_\infty \otimes \rho_p$$

The question remains the same[2], for <u>each</u> given p.

$\rightsquigarrow$ $(\infty \times p)$-adic viewpoint.

$SL_2(\mathbb{Z}[\frac{1}{p}])$ then appears as "arithmetic fundamental group".

---

1) Cf. [Stk], Satake's formulation was in terms of spherical functions and PL_2

2) To be precise, for $(R_j C_j)$ for level 1. For level $N \not\equiv 0(p)$, replace $SL_2(\mathbb{Z}[1/p])$ by its congruence subgr'p of level N.

I-2 By this restriction of scope (focusing):

Gain some new insights into
- ...,
- Towers of curves with many $\mathbb{F}_{q^2}$-rational points,
- Changing Quaternions, by Čerednik-Drinfeld,
- Darmon's work [Drm], ...

Out of focus
- Global aspects[1], including rel'ns with Quaternions; moduli, ℓ-adic representations.

Among them a non-obvious ℓ-adic counterpart is:

$$\prod_{\ell \neq p}{}' SL_2(\mathbb{Q}_\ell) \curvearrowright \Big(\prod_{\ell \neq p}{}' SL_2(\mathbb{Q}_\ell)\Big) \Big/ B_{\infty,p}^{(1)}$$

norm 1

the quaternion alg/$\mathbb{Q}$ ramified at ∞, p.

---

1) Names related include (Hecke, Weil, ... and)
Kronecker, Hasse, Witt, Deuring, Eichler, Igusa, ...
...supersingular moduli & quaternions (I-3 below)
Shimura ... Shimura curves < Shimura varieties
Serre, Deligne, Langlands, Drinfeld, ...:
(after Taniyama) ... ℓ-adic, adelic, ...

I-3 Celebration.

It is about 80 years since the discovery of "supersingular elliptic curves", specific but crucially basic objects in arithmetic geometry. Basic in the sense that they appear as a factor in every final specialization of abelian varieties. Historically, they appeared in full shape in a series of works, mainly by H.Hasse and M.Deuring, with the support of M.Eichler's work on the arithmetic of quaternion algebras over number fields. All during 1930-1941 in Germany. They survived, fortunately, having been published in local but internationally distributed Journals.

Before limiting ourselves to the (∞x p)-adic viewpoint, let us briefly recall their birth and celebrate their survival.1)2)

(Before Hasse) Some scattered examples of elliptic curves over $\bar{\mathbf{F}}_p$ with no points $\neq 0$ of order p might very well have been known.

---

1) My knowledge on this history is regrettably limited. The following description relies mainly on the Introduction in [Drg 1]. I hope that future students in arithmetic geometry will have more opportunities to learn and feel closer to these old but still fresh excitements of distinguished mathematicians in "Elliptische(..) Funktionenkörper(..)". These papers definitely contain something concrete and so beautiful that are not found in the standard textbooks in modern arithmetic geometry.

2) I heard from my colleague (in geophysics), of a saying "often a reseacher is strongly influenced by some paper published around the year of his (or her) birth". It applies to my case, too, and in more than one way.

(mid 1930's). H. Hasse, while working on the Riemann Hypothesis for elliptic curves/finite fields, first noticed that the endomorphism ring End(E) of some elliptic curve $E/\overline{\mathbb{F}}_p$ can be non-commutative, with $B = \mathrm{End}(E) \otimes \mathbb{Q}$ being a definite quaternion algebra$/\mathbb{Q}$, and also that such E can have no points $\neq 0$ of order p.[1]

He also discovered the Hasse-invariant of E, which is basically a polynomial of coefficients of the defining equation for E and whose vanishing is equivalent to the non-existence of such points. [HS1~2].

(1937~38) M. Eichler gave explicit class number formulas for quaternion algebras B/k over number fields, ending with the hardest case: k totally real, B totally definite, based on his "Mass Formula" [Ech]. (analytic).

(1941) M. Deuring [Drg 1, 2] gave a complete functorial description of

$$\begin{array}{ccccc} \overline{\mathbb{F}}_p & \approx & \text{elliptic curves over } \overline{\mathbb{F}}_p/\simeq & \twoheadrightarrow & \left\{\begin{matrix}\text{two types of}\\ \text{rings}\end{matrix}\right\} \\ j & \longmapsto & E_j & \longmapsto & \mathrm{End}(E_j) \\ & & \begin{matrix}\text{isogenies}\\ \text{among them}\end{matrix} & & \begin{matrix}\text{ideal transforms}\\ \text{of rings}\end{matrix} \end{array}$$

1) Deuring then noticed that B must be $B_{\infty,p}$.

Supersingular j

i.e. $\left(\text{Hasse inv}(E_j)=0 \right) \longleftrightarrow \text{End}(E_j) \simeq$ a maximal order $\mathcal{O}$ of $B_{\infty,p}$.

among them, $j \in \mathbb{F}_p \underset{1:1}{\longleftrightarrow} \mathcal{O}$ s.t. $\mathcal{O} \ni {}^{\exists}\alpha,\ N(\alpha)=p$, (up to conjugation)

$(j, j^p) \underset{2:1}{\longleftrightarrow} \mathcal{O}$ " $\mathcal{O} \not\ni \alpha,\ N(\alpha)=p$
$\quad\ \text{\rotatebox{90}{$\in$}}$
$\mathbb{F}_{p^2} \setminus \mathbb{F}_p$

In other words, $\#\{E \ ;\ \text{Hasse inv}(E)=0\} =$ the class number of $B_{\infty,p}$.
(up to $\simeq/\bar{\mathbb{F}}_p$)

Ordinary j I omit the (by-now-well known)[1] results of Deuring for this case. This includes a beautiful unique liftability of E together with the Frobenius π to characteristic 0, later generalized to ordinary abelian varieties (Serre-Tate).

In connection with the present subject, this was used for the proof of the Conjectures in II-2 below, for $\Gamma = PSL_2(\mathbb{Z}[\frac{1}{p}])$ ([6]~[8] CRV), while the lifting problem treated in VI is a "non-abelian version" of the Deuring's lifting of (E, π).

---

1) see Introductions in [Tt] (and also [5]) to see that it was not so well-known until mid 60's.

II Analogues of the Selberg ζ-function

II-1 M. Kuga drew my interest to the Selberg zeta function which is associated to each lattice $\Delta \subset PSL_2(\mathbb{R})$ [S86]. I looked for analogues for lattices in $PGL_2(k_\mathfrak{p})$ ($\mathfrak{p}$-adic field $N(\mathfrak{p})=q$) [4], and then for "irreducible" lattices in $PSL_2(\mathbb{R}) \times PGL_2(k_\mathfrak{p})$ w.r.t. primitive "∞-elliptic" conjugacy classes. To focus attention to connections with curves over $\mathbb{F}_{q^2}$, let us here restrict to discrete subgroups Γ of

$$PSL_2(\mathbb{R}) \times PGL_2^+(k_\mathfrak{p}) = \{g \in GL_2(k_\mathfrak{p});\ \mathrm{ord}_\mathfrak{p}(\det(g)) \equiv 0 \pmod 2\}/k_\mathfrak{p}^\times$$

with finite-volume quotients, which are "irreducible" $\longleftrightarrow$ $\overset{\text{top. closure}}{\overline{\mathrm{proj}_\mathbb{R}\Gamma}} = PSL_2(\mathbb{R})$ $\longleftrightarrow$ $\overline{\mathrm{proj}_\mathfrak{p}\Gamma} \supseteq PSL_2(k_\mathfrak{p})$.

The group $PSL_2(\mathbb{Z}[1/p])$ is such an example. Other Γ's arise from quaternion algebras over totally real number fields k which split at just one of the infinite primes and at a finite prime $\mathfrak{p}$ with which $k_\mathfrak{p}$ is the completion. As the group $\Gamma = PSL_2(\mathbb{Z}[1/p])$ describes some properties of modular curves at p, the quaternionic Γ describes properties at $\mathfrak{p}$ of Shimura curves.

◎ If $U \subset PGL_2^+(k_\mathfrak{p})$ is any open compact subgroup, then $\Gamma_U := \mathrm{proj}_\mathbb{R}(\Gamma \cap (PSL_2(\mathbb{R}) \times U))$ is a lattice in $PSL_2(\mathbb{R})$.

For simplicity, assume Γ : torsion-free.

◎ $\Gamma \ni \gamma = (\gamma_\infty, \gamma_\mathfrak{p})$: ∞-elliptic $\overset{}{\underset{\text{def}}{\Longleftrightarrow}}$ γ_∞ has imaginary eigenvalues.

◎ γ : ∞-elliptic $\Longrightarrow$ $\gamma_\mathfrak{p}$ has two distinct eigenvalues in $k_\mathfrak{p}^\times$.

$\left\{ \begin{array}{l} \text{its centralizer } \Gamma_\gamma \text{ is } \cong \mathbb{Z} \\ \{\gamma^{-1}\}_\Gamma \neq \{\gamma\}_\Gamma \end{array} \right.$ the Γ-conjugacy class

◎ An ∞-elliptic γ : called primitive, if it generates Γ_γ.

◎ $\mathrm{Primes}(\Gamma) = \{$ Pairs $(\{\gamma\}_\Gamma, \{\gamma^{-1}\}_\Gamma)$ of mutually inverse primitive ∞-elliptic Γ-conjugacy classes $\}$

$\mathrm{Primes}(\Gamma) \ni P = \{\gamma^{\pm 1}\}_\Gamma$

◎ $\deg P := \frac{1}{2} \left| \mathrm{ord}_\mathfrak{p}(\lambda_\mathfrak{p}' \lambda_\mathfrak{p}^{-1}) \right|$ (well-defined, $\in \mathbb{Z}, \geq 1$)

$\lambda_\mathfrak{p}, \lambda_\mathfrak{p}'$: eigenvalues of a matrix representation of $\gamma_\mathfrak{p}$.

◎
$$\zeta_\Gamma(u) := \prod_{P \in \mathrm{Primes}(\Gamma)} (1 - u^{\deg P})^{-1}$$

makes sense as a formal power series.

= a rational function of u of the form described below.

Computed [8] [Ih] $\Uparrow$

◎ Compare with the zeta function of a $\begin{pmatrix}\text{complete}\\ \text{smooth}\\ \text{abs. irred}\end{pmatrix}$ curve $\mathcal{X}/\mathbb{F}_{q^2}$;

$$\zeta_{\mathcal{X}}(u) = \prod_{P \in \underbrace{\mathrm{Primes}(\mathcal{X})}_{\text{closed points of } \mathcal{X}}} (1-u^{\deg P})^{-1}$$

$$= \frac{F_{\mathcal{X}}(u)}{(1-u)(1-q^2u)},$$

$F_{\mathcal{X}}(u) \in \mathbb{Z}[u]$, $\deg F_{\mathcal{X}} = 2g_{\mathcal{X}}$, $g_{\mathcal{X}}$: the genus.

◎ For simplicity, assume further that Γ is cocompact ($\leftrightarrow \Gamma_U$: cocompact)

To my surprise,

looks like, in form, for some $\mathcal{X}$

$$\boxed{\underbrace{\zeta_\Gamma(u)}_{\displaystyle \begin{array}{c}\| \\ \prod_{\mathrm{Primes}(\Gamma)} (1-u^{\deg P})^{-1}\end{array}} \times \{(1-u)^{-1}\}^{(q-1)(g_\Gamma-1)} \overset{?}{=} \begin{array}{c}\zeta_{\mathcal{X}}(u)\\ \| \\ \prod_{\mathrm{Primes}(\mathcal{X})} (1-u^{\deg P})^{-1}\end{array}}$$

Here, $g_\Gamma :=$ genus of $\Gamma_U \backslash \mathfrak{H}$, U: a maximal cpt subgrp[1] of $PGL_2^+(\mathbb{R})$

(cf [8] Ch I)

the complex upper half plane

1) There are two conjugacy classes in PGL_2^+, but as long as Γ is torsion-free, g_Γ does not depend on the choice of U (cf [8] Ch I §35)

So, I conjectured exactly what you would conjecture from this observation (late 1960's; [6]~[8]):

II-2

(A) Each Γ determines some curve $\mathfrak{X}/\mathbb{F}_{q^2}$, together with a set $\mathfrak{S}$ of $\mathbb{F}_{q^2}$-rational points, $|\mathfrak{S}| = (q-1)(g_{\mathfrak{X}}-1)$.

Moreover, the pair $(\mathfrak{X}, \overset{\text{conj.}/\mathbb{F}_q}{\mathfrak{X}'})$ is related to the pair $\left(\mathfrak{H}/\Gamma_U, \mathfrak{H}/\Gamma_{U'}\right)$ (U, U': mutually PGL_2-conj. but not PGL_2^+-conj. max. cpt subgrps) of complex curves, by "lifting-reduction" relations.

(B)
$$\begin{array}{ccc} \mathrm{Primes}(\Gamma) & \overset{\exists}{\longleftrightarrow} & \mathrm{Primes}(\mathfrak{X}) - \mathfrak{S} \\ \Psi & & \Psi \\ \{\gamma^{\pm 1}\}_\Gamma & & P \end{array}$$
a canonical deg-preserving bijection

(C)
$$\begin{array}{ccc} \Gamma^* & & \mathfrak{X}^* \supset \mathfrak{S}^* \\ \cap & \overset{\exists}{\longleftrightarrow} & \downarrow \quad\; \downarrow \\ \Gamma & & \mathfrak{X} \quad\; \mathfrak{S} \end{array}$$
subgrps with finite indices

the preimage

finite etale connected covers s.t. all pts of $\mathfrak{S}^*$ are $\mathbb{F}_{q^2}$-rat'l

(D) Depending on the choice of an "∞-p bridge," the sign of ∞-elliptic conj. class is defined, s.t. for each $\{\gamma^{\pm 1}\}_\Gamma$, just one of $\{\gamma\}_\Gamma$ is positive, and

$$\left.\begin{array}{l} \text{When } \Gamma^* \triangleleft \Gamma \text{ and} \\ \underset{\substack{\top \\ \text{positive}}}{\{\gamma\}_\Gamma} \underset{\text{by}(B)}{\longleftrightarrow} P \end{array}\right\} \text{ then } \left\{\begin{array}{l} \Gamma/\Gamma^* \xrightarrow{\sim} Gal(\mathfrak{X}^*/\mathfrak{X}), \text{ and} \\ \{\gamma\}_\Gamma \bmod \Gamma^* \leftrightarrow \left(\dfrac{\mathfrak{X}^*/\mathfrak{X}}{P}\right) \end{array}\right.$$

the Frobenius conj. class.

For a generalized formulation & details [cf: "Author's Notes 2008" in [8]].

I was excited (overly ?) thus:

Γ is "just as big as necessary". The Frobenius elements on the right-hand side (the arithmetic geometry side) are countable, so they must be parametrized by a discrete set. Adelic groups and conj. classes contain unnecessary elements. By replacing groups over $\prod_{\ell \neq p} \mathbb{Z}_\ell$ by those over $\mathbb{Z}[\frac{1}{p}]$, we obtained the "correct" left-hand side ..... Indeed, every ∞-elliptic Γ-conjugacy class finds its Frobenius power counterpart, and thus Γ must be called the arithmetic fundamental group for etale covers of $\mathfrak{X}$ in which pts. of $\mathfrak{S}$ split completely.!

II-3

This series of conjectures was later proved. For this, cf. "Author's Notes 2008" in [8].

In the beginning of 1970's I was trying to develop an $(\infty \times \mathfrak{p})$-adic method to give it its "eigen-proof". But soon Y. Morita (a graduate student) made an essential progress in the case of Shimura curves assoc. with quaternion algebras B/k (k: any totally real field), by combining Shimura theory[1] [Sh1][Sh2] with our $\zeta_\Gamma(u)$-results.[2] And on the other hand, G. A. Margulis proved the "arithmeticity" of lattices which include our $(\infty \times \mathfrak{p})$-adic lattices [Mrg1,2]. Probably, I should not have been discouraged, because development of method is more important. If sufficiently developed it could be applied to other problems too. At any rate, these conjectures were proved based on Shimura theory by collaboration of works of Morita, M. Ohta and myself (cf. loc. cit.), and I turned (1975) to the lifting problem, to find Γ starting from a given $(\mathfrak{X}, \mathfrak{S})$.

---

1) In Shimura's work, $\mathfrak{S}$ does not show up on the surface.

2) I had suggested him to work in the case $k = \mathbb{Q}$, which is more or less similar to the elliptic modular case, as his Master's thesis subject. Then, later in Princeton, Shimura strongly encouraged him to work on the general case where unexpected interesting things can be encountered! I understood that this was more reasonable.

V-4 The next basic questions (randomly ordered)

⊙ Which pair of $(\mathfrak{X}, \mathfrak{S})$ corresponds to some group Γ? Describe, explicitly, the condition for $(\mathfrak{X}, \mathfrak{S})$ to correspond to some Γ.

⊙ If $(\mathfrak{X}, \mathfrak{S})$ corresponds to some Γ arising from a quaternion algebra B/k, then B and $B_{\infty,p}$ must be hidden deep inside the datum $(\mathfrak{X}, \mathfrak{S})$. How can we see them?

⊙ Generalize "arithmetic fundamental groups"!

⊙ What <u>is</u> $\mathfrak{S}$?

(a) As the zeros of $(d\tau \,(\mathrm{mod}\, p))^{\otimes(p-1)}$ (cf. IV-6, V-3).

(b) If we consider the whole tower of $(\mathfrak{X}^*, \mathfrak{S}^*)$, and the full "non-compact" autom. grp $\mathcal{G}$ of the tower, then the projective system $\{\mathfrak{S}^*\}$ should form a single $\mathcal{G}$-<u>orbit</u>[1], with each stabilizer appearing as the lattice $\underline{(B_{\infty,p})_k^\times} \subset \mathcal{G} \simeq \prod'_{l \neq p} B_l^\times \cong \prod'_{l \neq p} (B_{\infty,p})_l^\times$

1) In this sense, the "essential cardinality" of $\mathfrak{S}$ is ONE, for each family in the category of covers.

II-5 Motivation from Igusa's remark [Ig1]

$$X = \mathbb{P}^1 \setminus \{0, 1, \infty\} : \quad \text{the } \lambda\text{-line.}$$

λ parametrizes the elliptic curve $E_\lambda : y^2 = x(x-1)(x-\lambda)$.

$X_{\mathbb{C}} = \Delta \backslash \mathfrak{H}$, $\quad \Delta$: the principal congruence subgr'p mod 2 of $PSL_2(\mathbb{Z})$.

Let $p \neq 2$ and Γ : the principal congruence subgr'p mod 2 of $PSL_2(\mathbb{Z}[\frac{1}{p}])$.

$$\Gamma \rightsquigarrow \begin{cases} \mathfrak{X} = \mathbb{P}^1 \setminus \{0,1,\infty\} / \mathbb{F}_{p^2} \\ \mathfrak{S} = \{\lambda_0 \,;\, E_{\lambda_0} : \text{supersingular}\} = \text{the zeros of } f(\lambda) = \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i}^2 \lambda^i \end{cases}$$

$$|\mathfrak{S}| = (p-1)(g_\Gamma - 1 + \tfrac{\#\,\text{cusps}}{2}) \underset{\text{here}}{=} \tfrac{1}{2}(p-1).$$

As Deuring explains in [Drg 1],

$$\#\{\text{supersingular moduli } j_0\} = \text{the class number of } B_{\infty,p} \underset{\uparrow}{=} \frac{p-1}{12} \pm \cdots$$

Eichler formula

$$\#\{\text{supersingular moduli } \lambda_0\} = \frac{p-1}{2} = \deg f(\lambda).$$

(1958) (1941)

Igusa [Ig 1] noticed that this simplicity of zeros of $f(\lambda)$ can be proved directly by using

Deuring's remark:
all zeros of $f(\lambda)$ must be simple;
with a comment "Dies unmittelbar dem Ausdruck $f(\lambda) = \cdots$ anzusehen scheint nicht leicht"
$\quad = \cdots$ above

[The Differential Equation over $\mathbb{F}_p$]:

$$\lambda(1-\lambda) f'' + (1-2\lambda) f' - \tfrac{1}{4} f = 0.$$

Trying to understand and generalize this "$(\infty \times p)$-adically," I noticed.

(a) the differential $\omega_0^{\otimes(p-1)} = \dfrac{f(\lambda)^2}{(\lambda(1-\lambda))^{p-1}} (d\lambda)^{\otimes(p-1)}$

of order $(p-1)$ is more intrinsic than $f(\lambda)$ itself;

(b) the Schwarzian differential equation whose solutions are

ratios of two independent solutions of

$$(\#) \qquad \lambda(1-\lambda)f'' + (1-2\lambda)f' - \frac{1}{4}f = 0$$

(say, over $\mathbb{C}$) should be more intrinsic than $(\#)$ itself.

$$\boxed{\text{The parameter } \tau \text{ of the complex upper half plane } \mathfrak{H} \text{ is such a ratio}}$$

(a) $\longrightarrow$ the associated differential (IV ~ VI) $\longrightarrow$ the lifting problem (VII).

(b) $\longrightarrow$ the Schwarzian (S-) operators (IV)

III Geometric objects $\bullet\swarrow\overset{\bullet}{}\searrow\bullet$ inbetween Γ and $(X, \mathfrak{S})$

III-1 From Γ-side.

Let $U = PGL_2(\mathcal{O}_\mathfrak{p})$, $U' = \begin{pmatrix}\pi & 0\\ 0 & 1\end{pmatrix}^{-1} U \begin{pmatrix}\pi & 0\\ 0 & 1\end{pmatrix}$ ($\pi \in k_\mathfrak{p}$, a prime elt), and $U^0 = U \cap U'$. Then the lattices $\Gamma_U, \Gamma_{U'}, \Gamma_{U^0}$ of $PSL_2(\mathbb{R})$ act on $\mathfrak{H} \doteq \{\tau \in \mathbb{C};\ \mathrm{Im}(\tau) > 0\}$ giving a system over $\mathbb{C}$;

$$
\begin{tikzcd}[column sep=small]
 & \Gamma_{U^0}\backslash\mathfrak{H} \arrow[dl] \arrow[dr] & \\
\Gamma_U\backslash\mathfrak{H} & & \Gamma_{U'}\backslash\mathfrak{H}
\end{tikzcd}
\quad \xrightarrow[\text{algebraize}]{\sim} \quad
\begin{tikzcd}[column sep=small]
 & X^0_\mathbb{C} = \text{“}T(\mathfrak{p})_\mathbb{C}\text{”} \arrow[dl, "\varphi_\mathbb{C}"'] \arrow[dr, "\varphi'_\mathbb{C}"] & \\
X_\mathbb{C} & & X'_\mathbb{C}
\end{tikzcd}
$$

(normalization of the graph of the Hecke correspondence $T(\mathfrak{p})$)

($\deg \varphi_\mathbb{C} = \deg \varphi'_\mathbb{C} = q+1$); Functorial equivalence:

$$
\begin{array}{c} \Gamma^* \\ \cap \\ \Gamma \end{array} \ \text{fin. index} \quad \longleftrightarrow \quad
\begin{tikzcd}
\mathcal{O} \arrow[d] & \mathcal{O} \arrow[l] \arrow[r] \arrow[d] & \mathcal{O} \arrow[d] \\
X_\mathbb{C} & X^0_\mathbb{C} \arrow[l] \arrow[r] & X'_\mathbb{C}
\end{tikzcd}
$$

Compatible system of fin. connected vertically etale covers

The key point for this equivalence was

$$PGL_2^+(k_\mathfrak{p}) = U \underset{U^0}{*} U' \quad (\underline{\text{free}} \text{ product with amalgamation});$$

$$\therefore \quad \Gamma = \Gamma_U \underset{\Gamma_{U^0}}{*} \Gamma_{U'} \quad ([4],\ [8]\ \mathrm{Ch}2,\ [12], \text{ also Serre } [Ser3]).$$

III-2 From $(\mathscr{X},\mathfrak{S})$-side.[1]

$$\left\{\begin{array}{l} \mathscr{X} : \text{a curve}/\mathbb{F}_{q^2}, \\ \mathfrak{S} \subseteq X(\mathbb{F}_{q^2}),\ \mathfrak{S} \neq \emptyset \end{array}\right.$$

Let $\mathscr{X}'$: the conjugate of $\mathscr{X}/\mathbb{F}_q$,

Π (resp. Π') the locus of (geom.) pts (x, x^q) (resp. (x'^q, x')) <u>on $\mathscr{X}\times\mathscr{X}'$</u>.

So, Π, Π' meet each other at $\{(x, x^q);\ x^{q^2}=x\}$, i.e., above each pt of $\mathscr{X}(\mathbb{F}_{q^2})$.

Let them cross as it is if $x\in\mathfrak{S}$, separate them ($\underset{\mathscr{X}\times\mathscr{X}'}{\text{outside}}$) if $x\notin\mathfrak{S}$.

$$\begin{tikzcd}
 & \mathscr{X}^0_{\mathfrak{S}} = \Pi \underset{\mathfrak{S}}{+} \Pi' \arrow[dl, "\varphi"'] \arrow[d] \arrow[dr, "\varphi'"] & \\
\mathscr{X} & \Pi \cup \Pi' \arrow[l, "pr_1"'] \arrow[r, "pr_2"] & \mathscr{X}'
\end{tikzcd}$$

$$\mathfrak{X} := \{\mathscr{X} \xleftarrow{\varphi} \mathscr{X}^0_{\mathfrak{S}} \xrightarrow{\varphi'} \mathscr{X}'\}$$

Compatible system of finite connected vertically-etale covers

$$\begin{tikzcd}
\mathscr{X}^* \arrow[d] & \bigcirc \arrow[l] \arrow[r] \arrow[d] & \mathscr{X}'^* \arrow[d] \\
\mathscr{X} & \mathscr{X}^0_{\mathfrak{S}} \arrow[l] \arrow[r] & \mathscr{X}'
\end{tikzcd}
\quad \longleftrightarrow \quad
\begin{tikzcd}
\mathscr{X}^* \arrow[d] \\
\mathscr{X}
\end{tikzcd}$$

fin. etale conn s.t. all pts above $\mathfrak{S}$ are again $\mathbb{F}_{q^2}$-rational

(Recall: "etale" above a double pt. on $\mathscr{X}^0_{\mathfrak{S}}$ implies "flat"; thence cannot separate a double point below into two points above.)

◎ This is a <u>geometric</u> interpretation of splitting of rational points of curves over $\mathbb{F}_{q^2}$

---

1) cf. [12] §4

III-3

Any object, with

one foot on the other foot on

$\{X_{\mathbb{C}} \leftarrow X^0_{\mathbb{C}} \rightarrow X'_{\mathbb{C}}\}$ $\{\mathfrak{X} \leftarrow \mathfrak{X}^0_{\mathfrak{S}} \rightarrow \mathfrak{X}'\}$

will be called a $\boxed{\text{Bridge}}$

[Bridge-Games]

(i) Construction from the Left. The greatest contributions after Kronecker are by Shimura [Sh1, 2] (1967, 70). They give $T(\mathfrak{p}) \equiv *\cdot\Pi + *\cdot{}^t\Pi$ in general forms, for each Shimura curve (say), for "almost all $\mathfrak{p}$". For the references related to results for individual $\mathfrak{p}$, the $\mathfrak{p}$-canonical model and "$(\infty\times\mathfrak{p})^{**}$-adic focusing", cf [18] §4 [47] §4.

(ii) Develop a theory, assuming the existence of a "bridge" (without assuming that $\mathcal{X}_{\mathbb{C}}$ comes from some $(\infty\times\mathfrak{p})$-adic Γ).

For this, cf. [18][19] (mid 1970's)

(iii) Trials for Constr. from the Right (the "lifting problem")

[17][20] (late 1970's), plus "recent alpha" (Ch VI; below)

IV Schwarzian operators and Frobenius-associated differentials.

IV-0 Introduction

Whenever there is a bridge connecting a system $\{X_{\mathbb{C}} \leftarrow X^0_{\mathbb{C}} \rightarrow X'_{\mathbb{C}}\}$ of complex algebraic curves and $\{\mathfrak{X} \leftarrow \mathfrak{X}^0_{\mathfrak{S}} \rightarrow \mathfrak{X}'\}$ of algebraic curves over $\mathbb{F}_{q^2}$ (III 1~3), we (shall) have:

[$\mathbb{C}$-side] $(i)_{\mathbb{C}}$ simultaneous τ-uniformization;

$(ii)_{\mathbb{C}}$ the family of differentials $\left\{d\left(\frac{A\tau+B}{C\tau+D}\right);\ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in GL_2(\mathbb{C})\right\}$;

$(iii)_{\mathbb{C}}$ $\exists$ an algebraic diffential operator "on $\{X_{\mathbb{C}} \leftarrow X^0_{\mathbb{C}} \rightarrow X'_{\mathbb{C}}\}$,"

$$S_{can} : \{\text{Differentials}\} \underset{\sigma}{\nrightarrow} \{\text{Quadratic differentials}\},$$

s.t. $\quad \mathrm{Ker}(S_{can}) = $ the family $(ii)_{\mathbb{C}}$;

$(iv)_{\mathbb{C}}$ $\quad S_{can}$ can be characterized algebraically.

[p-adic side w.r.t. any formal p-adic lifting of $\{\mathfrak{X} \leftarrow \mathfrak{X}^0_{\mathfrak{S}} \rightarrow \mathfrak{X}'\}$]

$(0)_p$ $\exists_1$ formal lifting σ of the q-th power morphism;

$(iv)_p$ $\quad \exists_1$ σ-invariant "S-operator" $\mathfrak{S}$,

$(ii)_p$ $\quad \exists_1$ a p-adic diffenential ω, s.t. $\omega^{\sigma-1}$ = a constant, called the σ-associated differential ($\exists_1$ up to constant multiples). (ω is "multi-valued"; it lives in an infinite tower of p-unram. covers).

$(iii)_p$ $\quad \mathrm{Ker}(\mathfrak{S}) = \{\text{constant multiples of } \omega\}$.

$(V)_p$ Moreover, when $|\mathfrak{S}| = (q-1)(g_{\mathfrak{X}}-1)$, the differential $\omega_0 = \omega \pmod{\mathfrak{g}}$ has the property:

$\omega_0^{\otimes(q-1)}$ is a regular differential on $\mathfrak{X}$ of order $q-1$, with the divisor $(\omega_0^{\otimes(q-1)}) = 2\mathfrak{S}$.

[When a bridge (III-3) exists] The comparison theorem (IV-6) asserts "$S_{can} = \mathbb{S}$" on any given bridge, thus

[(∞, p) comparisons]

◎ $\left\{ d\left(\frac{A\tau+B}{C\tau+D}\right) \right\} \longleftrightarrow \left\{ c\omega, \ c: \text{constant} \neq 0 \right\}$

◎ $S_{can} \longleftrightarrow \mathbb{S}$.

...

[$\infty \to p$]: Starting from Γ, $\mathfrak{S}$ can be reached, first by looking at the canonical S-operator on the ∞-side associated with τ-uniformization, then by using algebraicity and the comparison theorem pass to the p-adic side, then to the mod p solution ω_0, then to the divisor of $\omega_0^{\otimes(p-1)}$ which is $2\mathfrak{S}$.

[$p \to \cdots \to \infty$] Starting from $\{\mathfrak{X} \leftarrow \mathfrak{X}^{\circ}_{\mathfrak{S}} \to \mathfrak{X}'\}$, the associated differential mod p^n plays a crucial role in the problem of liftings of the system mod p^{n+1} (see VI).

We begin this Ch IV with the definition of S-operators.

IV-1 Schwarzian derivatives and S-operators [1]

(1) $K \supsetneq k$: fields, $D(K)$: a 1-dim. K-module,

$$d : K \to D(K) : \begin{cases} \text{a differentiation, i.e., additive;} \\ d(xy) = x\,dy + y\,dx \quad (x, y \in K) \end{cases}$$

$k = \mathrm{Ker}(d)$. Put

$$D^0(K) = K, \quad \underset{(h \geq 1)}{D^h(K) = D(K)^{\otimes h}} \quad (\otimes \text{ over } K).$$

(2) For $\xi, \eta \in D(K) \setminus \{0\}$, the Schwarzian derivative $\langle \eta, \xi \rangle \in D^2(K)$ is defined by

$$\langle \eta, \xi \rangle = \frac{2w_1w_3 - 3w_2^2}{w_1^2}\, \xi^{\otimes 2}$$

$$\underset{2)}{=} d\log w_1 \otimes d\log (w_2^2 w_1^{-3}),$$

where $\quad w_1 = \eta/\xi, \quad w_{i+1} = dw_i/\xi \quad (i \geq 1) \quad \in K,$

$$d\log w := dw/w \in D(K).$$

(3) $\langle \eta, \xi \rangle$ is not bilinear but "behaves like $\eta - \xi$," i.e.,

$$\langle \eta, \zeta \rangle - \langle \xi, \zeta \rangle = \langle \eta, \xi \rangle.$$

In particular, $\quad \langle \eta, \eta \rangle = 0, \quad \langle \xi, \eta \rangle = -\langle \eta, \xi \rangle.$

Also, $\quad \langle \eta, \xi \rangle = \langle c\eta, c'\xi \rangle \quad \forall c, c' \in k^\times.$

---

1) cf. [13], or [8] Ch. 2

2) This 2nd expression is helpful; e.g. when K/k is an algebraic function field of 1-var and $\mathfrak{P}$ is any place, then $\mathrm{ord}_{\mathfrak{P}}\, d\log w \geq -1$; hence $\mathrm{ord}_{\mathfrak{P}} \langle \eta, \xi \rangle \geq -2$, as can be seen directly.

(4) For a fixed ξ,

$$\eta \text{ satisfies } \langle \eta, \xi \rangle = 0 \iff \begin{cases} \text{(i) when } \xi = dx \ (\exists x \in K), \\ \quad \eta = d\left(\frac{Ax+B}{Cx+D}\right),\ \exists \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in GL_2(k). \\ \text{(ii) When otherwise,} \\ \quad \eta = c\,\xi, \quad \exists c \in k^\times. \end{cases}$$

(5) A map

$$\mathcal{S} : D(K) \setminus \{0\} \longrightarrow D^2(K)$$

is called an $\mathcal{S}$-operator on K, if

$$\mathcal{S}\langle \eta \rangle - \mathcal{S}\langle \xi \rangle = \langle \eta, \xi \rangle \qquad \forall \eta, \xi \in D^1(K) \setminus \{0\}.$$

(Note that the difference between two $\mathcal{S}$-operators is a constant $\in D^2(K)$.

(6) For any fixed $\zeta \in D^1(K) \setminus \{0\}$,

$$\mathcal{S}_\zeta : \eta \longmapsto \langle \eta, \zeta \rangle$$

is an $\mathcal{S}$-operator (by (3)), called the <u>inner</u> $\mathcal{S}$-operator w.r.t. ζ.
All other $\mathcal{S}$-operators are of the form $\mathcal{S} = \mathcal{S}_\zeta + C$ (C: a constant $\in D^2(K)$).

An $\mathcal{S}$-operator on K is inner w.r.t ζ if and only if

$$\mathcal{S}\langle \zeta \rangle = 0.$$

IV-2 The canonical S-operator S_{can} ($\mathbb{C}$-side)

Let $\Delta \subset PSL_2(\mathbb{R})$ be a lattice subgroup, i.e., discrete, $\mathrm{vol}(\Delta \backslash PSL_2(\mathbb{R})) < \infty$. This gives

$$\mathfrak{Z} = \{\tau \in \mathbb{C} ;\ \mathrm{Im}(\tau) > 0\} \longrightarrow \Delta \backslash \mathfrak{Z} = X_{\mathbb{C}} : \text{an alg. curve}/\mathbb{C} ;$$

$$\tilde{K} = \left\{ \begin{matrix} \text{meromorphic} \\ \text{fctns}^{1)} \text{ on } \mathfrak{Z} \end{matrix} \right\} \supset \underset{\substack{\vdots \\ \Delta\text{-invariant} \\ \text{elts}}}{\tilde{K}^{\Delta}} = K = \left\{ \begin{matrix} \text{rational} \\ \text{fctns on } X_{\mathbb{C}} \end{matrix} \right\}.$$

Consider the inner S-operator.

$$\begin{array}{cccc} S_{d\tau} : & D(\tilde{K}) \setminus \{0\} & \longrightarrow & D^2(\tilde{K}) \quad \text{on } \tilde{K}. \\ & \eta & \longmapsto & \langle \eta, d\tau \rangle. \end{array}$$

For $\delta \in \Delta$, $\langle \eta, d\tau \rangle^{\delta} = \langle \eta^{\delta}, d(\tau^{\delta}) \rangle = \langle \eta^{\delta}, d\tau \rangle$. ($\tau^{\delta}$: lin. fractional transf. of τ) So, if $\eta \in D(K)$, then $\langle \eta, d\tau \rangle$ is Δ-invar.; hence $\in D^2(K)$. Thus, $S_{d\tau}$ induces an S-operator

$$D(K) \setminus \{0\} \longrightarrow D^2(K) \quad \underline{\text{on } K},$$

called the canonical S-operator S_{can} (w.r.t. Δ).

As an S-operator on K, S_{can} is <u>not</u> inner.

The extension $\tilde{K}$ of K <u>makes</u> the unique (analytic) extension of S_{can} on $\tilde{K}$ <u>inner</u>.

---

1) When $\Delta \backslash \mathfrak{Z} \neq$ compact, need additional (well-known) conditions at cusps.

[<u>An algebraic characterization of</u> $\check{S}_{can}$!] ([8] Ch 2 §§41,45)

(1) k: any field of char. 0, L/k: a 1-dimensional extension s.t.

$(L0)_k$ k is algebraically closed in L;

$(L1)_k$ "Almost unramified," i.e.,

$$\mathcal{L}_0 := \{ L_0 ;\ \underbrace{k \subset L_0}_{\substack{\text{finitely}\\\text{generated}\\\text{ext'n}}} \underbrace{\subseteq L}_{\substack{\text{normal algebraic ,}\\\text{unram. outside a}\\\text{finite set of primes of } L_0/k}} \} \neq \phi ;$$

$(L2)_k$ "General type"; i.e.,

$$\exists L_0 \in \mathcal{L},\ \text{genus}(L_0) > 1;$$

$(L3)_k$ "Ample", i.e.,

$$\exists L_0, L_0' \in \mathcal{L}_0 , \quad L_0 \cap L_0' = k;$$

equivalently, <u>the automorphism group</u> $\mathrm{Aut}(L/k)$ is <u>non</u>-compact.
(under Krull topology)

When $k = \mathbb{C}$, system of curves corresponding to $\mathcal{L}_0$ defines a simultaneous uniformization by $\mathfrak{H}$, and hence the canon. S-operator on L makes sense.

---

(2) The group $\mathrm{Aut}(L/k)$ acts on the set of S-operators $\{S\}$ on L (w.r.t. the standard differentiation over k), by

$$(S^\rho)\langle\eta\rangle = (S\langle\eta^{\rho^{-1}}\rangle)^\rho , \qquad (\rho \in \mathrm{Aut}(L/k)).$$

<u>Theorem IV-2 ([8]Ch 2, Th 9,10)</u> (i) There exists a unique $\mathrm{Aut}(L/k)$-invariant S-operator S^{inv} on L. (ii) If $\iota : k \hookrightarrow \mathbb{C}$ is any field embedding, S^{inv} corresponds to S_{can} of $L \otimes_{k,\iota} \mathbb{C}$.

<u>Remark</u> If $k_0 \subset k$ with k/k_0 algebraic, $\tilde{\rho} \in \mathrm{Aut}(L/k_0)$, then S^{inv} is also $\tilde{\rho}$-invariant, because $k^{\tilde{\rho}} = k$ and hence $\tilde{\rho}$ normalizes $\mathrm{Aut}(L/k)$.

<u>IV-3</u> <u>The Frobenius-invariant S-operator $\mathbb{S}$</u> (<u>p-adic side</u>)

(1) Let $\{K/k, D(K), d\}$ be as in IV-1. Suppose further:

$$\left\{\begin{array}{l} K \text{ is equipped with an additive normalized discrete valuation} \\ \qquad\qquad \mathrm{ord} : K^{\times} \to \mathbb{Z} \\ \text{of unequal characteristics } (0, p), \text{ s.t.} \\ \quad \text{i) } \; d : K \to D(K) \text{ is continuous, ii) } \mathrm{ord}(k^{\times}) = \mathbb{Z}. \end{array}\right.$$

Denote by Θ (resp. θ) the valuation ring in K (resp. k) and by $\mathbb{K}$ (resp. κ) the residue field of K (resp. k).

(2) By (1), $\Theta d\Theta \subset D(K)$ is a free Θ-module of rank 1, and

$$\bar{d}: \mathbb{K} \longrightarrow D(\mathbb{K})$$

is induced. (As $\mathrm{char}(\mathbb{K}) = p$, $\mathrm{Ker}(\bar{d})$ contains $\mathbb{K}^p$.)

(3) $\mathrm{ord}: K^\times \to \mathbb{Z}$ extends uniquely to

$$\mathrm{ord}: \bigcup_{h \geq 0} (D^h(K) \setminus \{0\}) \longrightarrow \mathbb{Z}, \qquad \text{s.t}$$

$$\begin{cases} \text{(i)} & \mathrm{ord}(\zeta) = 0 \quad \text{if} \quad \Theta d\Theta = \Theta \zeta, \\ \text{(ii)} & \mathrm{ord}(\xi \otimes \eta) = \mathrm{ord}(\xi) + \mathrm{ord}(\eta) \quad \forall \xi, \eta \text{ on the left side.} \end{cases}$$

(4) An element $\xi \in D^h(K)$ is called <u>integral</u>, if $\mathrm{ord}(\xi) \geq 0$ (or $\xi = 0$).

- For any $w \in K^\times$, $d\log w$ is integral. ($\because$ can assume $\mathrm{ord}(w) = 0$ by taking a $\mathbb{K}^\times$-multiple.)
- Hence $\langle \eta, \xi \rangle \in D^2(K)$ is integral.

(by the second expression for $\langle \eta, \xi \rangle$)

(5) Let $q = p^f$ ($f \geq 1$). A <u>q-th Frobenius</u> (map) <u>of</u> K is a value-preserving homomorphism

$$\sigma: K \longrightarrow K^\wedge$$

into the completion $K^\wedge$, s.t.

$\{$ (i) σ induces the q-th power map of the residue field $\mathbb{K}$, and

(ii) σ commutes with the differentiation d, i.e., $dx = 0 \Leftrightarrow d(x^\sigma) = 0$ and $(dy/dx)^\sigma = d(y^\sigma)/d(x^\sigma)$ ($\forall x, y \in K$ s.t. $dx \neq 0$). Thus σ induces uniquely a covariant homomorphism of modules $D^h(K) \to D^h(K^\wedge)$, denoted also by σ.

(6) Let K be complete. The different exponent $\nu = \nu_\sigma$ of σ is the unique <u>positive</u> integer satisfying

$$\mathrm{ord}(\xi^\sigma) = \mathrm{ord}(\xi) + h\nu \qquad \left(\begin{matrix} \forall \xi \in D^h(K) \setminus \{0\} \\ (h \geq 1) \end{matrix} \right).$$

(7) An S-operator on K is called <u>integral</u> if $S\langle\xi\rangle$ is integral. Since $\langle\eta, \xi\rangle$ is always integral, $S\langle\xi\rangle$ is integral for all ξ if so for one ξ.

(8) Let K be complete, $\sigma: K \to K$ a q-th Frobenius. An S-operator S on K is called <u>σ-invariant</u> if $(S\langle\eta\rangle)^\sigma = S\langle\eta^\sigma\rangle$ holds for all $\eta \in D(K) \setminus \{0\}$.

<u>Theorem IV-3([Ih][Kh])</u> There exists a unique σ-invariant S-operator $\mathbb{S}$ on K. It is integral.

(∵) Fix any $\zeta \in D(K) \setminus \{0\}$, $C \in D^2(K)$. Then $S = S_\zeta + C$ is σ-invar. $\Longleftrightarrow$ $C - C^\sigma = \langle \zeta, \zeta^\sigma \rangle \Leftrightarrow C = \sum_{n=0}^{\infty} \langle \zeta, \zeta^\sigma \rangle^{\sigma^n}$. Note here that the only σ-invar. elt of $D^2(K)$ is 0. //

IV-4 The differential ω associated with a Frobenius σ, and the equation $\mathfrak{S}\langle \omega \rangle = 0$.

(1) Notations being as in IV-3, we further assume:

◎ K: complete, $\sigma: K \to K$ a q-th Frobenius,

$$\left\{ \begin{array}{l} k \overset{\exists}{\supseteq} k_\mathfrak{p} \text{ a } \mathfrak{p}\text{-adic field, } \mathfrak{p} = (\pi), \text{ with } N(\mathfrak{p}) = q,\ \mathrm{ord}(\pi) = 1, \\ \qquad \sigma|_{k_\mathfrak{p}} = \text{identity}. \end{array} \right\}$$

Let $\tilde{K}$: the completion of the maximum unramified ext'n of K, so that $\mathrm{Aut}(\tilde{K}/K) \simeq \mathrm{Gal}(\mathbb{K}^{sep}/\mathbb{K})$. Then σ extends uniquely to a q-th Frobenius of $\tilde{K}$, and each S-operator S on K also extends uniquely to that on $\tilde{K}$.[1)]

(2)

Theorem IV-4(A)[1*)] There exists a differential $\omega \in D(\tilde{K})$ with $\mathrm{ord}(\omega) = 0$ such that

$$\omega^\sigma = \pi^\nu \omega \qquad (\nu = \nu_\sigma).$$

Such an ω is unique up to $\mathcal{O}_\mathfrak{p}^\times$-multiples ($\mathcal{O}_\mathfrak{p}$: the ring of integers of $k_\mathfrak{p}$).

---

1) We shall use the same symbols σ, S for these unique extensions (instead of denoting them like $\tilde{\sigma}$, $\tilde{S}$).

1)* = 1) for the next page

This is the differential associated with σ (w.r.t. π).

(3)

<u>Theorem IV-4 (A')</u>[1)] There exists a continuous character

$$\chi : \quad Gal(\mathbb{K}^{sep}/\mathbb{K}) \longrightarrow \mathcal{O}_{\mathfrak{p}}^{\times},$$

s.t.

$$\omega^{\tilde{\tau}} = \chi(\tau)\,\omega$$

for any $\tau \in Gal(\mathbb{K}^{sep}/\mathbb{K})$ and the corresponding $\tilde{\tau} \in Aut(\tilde{K}/K)$.

We shall denote by $\mathbb{K}(\omega)$ the abelian ext'n $/\mathbb{K}$ corresponding to $Ker(\chi)$, although ω does not belong to this field of char. p but to the corresponding subext'n of $\tilde{K}$, to be denoted as $K(\omega)$.

(4)

<u>Theorem IV-4 (B)</u>[1)] The unique σ-invariant S-operator $\mathcal{S}$ on K, when extended to an S-operator on $\tilde{K}$, becomes an inner S-operator w.r.t the σ-associated differential ω;

$$\mathcal{S}\langle\omega\rangle = 0$$
$$\mathcal{S}\langle\eta\rangle = \langle\eta, \omega\rangle \qquad \forall \eta \in D(\tilde{K}) \setminus \{0\}.$$

---

1) For the proofs, cf. [17] §9 (mod $\mathfrak{p}^{n+1}$-truncated version, constituting the main point of proof); or [Ih], for a formal p-adic version.

(5)

The reduced associated differential $\omega_0 = \omega \pmod{\mathfrak{p}}$

This is a differential $\omega_0 \in D(\mathbb{K}^{sep})$ s.t. $\omega^{\otimes(q-1)} \in \overset{q-1}{D}(\mathbb{K})$,

which may be expressed as

$$(*) \qquad \omega_0^{\otimes(q-1)} = \frac{\xi_0^{\otimes(q-1)}}{(\pi^{-\nu}(\xi^\sigma/\xi))_0} \in \overset{q-1}{D}(\mathbb{K})$$

(ξ : any elt of $D(\mathbb{K})$ with ord.$(\xi) = 0$, and $*_0 := * \pmod{\mathfrak{p}}$)

For ω_0, cf. [9] [14], and Appendix of [62] for a generalized treatment.

(6) Prop IV-4 If $q = p = \pi$ and $\mathbb{K}$ is either a function field of one variable$/k$, or $\simeq k((x))$, (k: a finite ext'n$/\mathbb{F}_p$), then $\nu = 1$ and ω_0 is log-exact.

(∵) Take any $t_0 \in \mathbb{K}$, $dt_0 \neq 0$, and $t \in K$ s.t. $t \equiv t_0 \bmod p$.

Put $t^\sigma = t^p + pr$. Then $p^{-1}(dt^\sigma/dt) \equiv t_0^{p-1} + dr_0/dt_0$

which cannot vanish; hence $\nu = 1$, and by (5)(*),

$$\omega_0^{\otimes(p-1)} = \frac{(dt_0)^{\otimes(p-1)}}{t_0^{p-1} + dr_0/dt_0};$$

i.e.,

$$\omega_0 = \left(\frac{\omega_0}{dt_0}\right)^p (t_0^p \, d\log t_0 + dr_0);$$

hence if γ denotes the Cartier operator on $D(\mathbb{K})$,

$$\gamma(\omega_0) = \frac{\omega_0}{dt_0} dt_0 = \omega_0; \text{ hence } \omega_0 \text{ is log-exact.} \quad //$$

IV-5 Each lifting $\mathfrak{X}$ of $\mathfrak{X}_0=\{\mathbb{X}\leftarrow \mathbb{X}^0_{\mathfrak{S}}\rightarrow \mathbb{X}'\}$ gives rise to $\sigma, \omega, \mathfrak{S}$.

(1) [$\mathfrak{p}$-adic] $k_{\mathfrak{p}}$: a $\mathfrak{p}$-adic field, $\mathcal{O}_{\mathfrak{p}}$: the valuation ring,
π : a prime element, $q=N(\mathfrak{p})$; $\mathcal{O}_{\mathfrak{p}}/\pi=\mathbb{F}_q$.

Let $\mathfrak{X}_0=\{\mathbb{X}\leftarrow \mathbb{X}^0_{\mathfrak{S}}\rightarrow \mathbb{X}'\}$ (III-2; $|\mathfrak{S}|=(q-1)(g_*-1)$),

$\mathfrak{X}=\{X \xleftarrow{\varphi} X^0 \xrightarrow{\varphi'} X'\}$: a symmetric lifting of $\mathfrak{X}_0$ over $\mathcal{O}_{\mathfrak{p}}$

proper flat$/\mathcal{O}_{\mathfrak{p}}$

in "the reasonable sense". ("symmetric unramified CR-system" in the sense of [18] §1; "unramifiedness" refers to that of $\varphi\otimes k_{\mathfrak{p}}$, $\varphi'\otimes k_{\mathfrak{p}}$, but these are equivalent with $|\mathfrak{S}|=(q-1)(g_*-1)$; hence satisfied in our situation)

The function fields:

$$\begin{array}{ccc} & K^0 & \\ K\nearrow & & \nwarrow K' \\ & K \xrightarrow{\sim} K' & \end{array}$$

of $\{X\leftarrow X^0\rightarrow X'\} = \mathfrak{X}$ are equipped with discrete valuations corresp. to

$$\begin{array}{ccc} & \Pi & \\ \mathbb{X} & & \mathbb{X}' \end{array}$$

$$\begin{array}{ccc} & v^0 & \\ v & & v' \end{array}$$

The conjugation isomorphism $K \xrightarrow{\sim} K'$ looked at v^0-adically induces a q-th Frobenius $\sigma: K^{\wedge} \rightarrow \hat{K}' \subset \hat{K}^0 = K^{\wedge}$ ($\wedge$: the v^0-adic completion) of $K^{\wedge}$.

(We note that ν_{σ} = the different-exponent of v^0/v').

(2) (cf. [18][19]) Let L : the simultaneous Galois closure of $K \diagup^{K^0} \diagdown K'$; i.e., the smallest Gal. ext'n $/K^0$ which is Galois $/K, K'$. It is actually an infinite extension. Call

$$\begin{tikzcd}
 & L \arrow[d, dash, "V^0"] \arrow[ddl, dash, bend right, "V"'] \arrow[ddr, dash, bend left, "V'"] & \\
 & K^0 \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] \arrow[rr, phantom, "G_{\iota^0}"] & & K' \arrow[dl, dash] \\
 & k_{\mathfrak{p}} &
\end{tikzcd}$$

V, V', V^0 : the Galois groups.

$G_{\mathfrak{p}}^{+} = \langle V, V' \rangle \overset{\text{open}}{\subset} \mathrm{Aut}(L/k_{\mathfrak{p}})$ generated by V, V' (actually non-compact) $= V \underset{V^0}{*} V'$ (free, with amalgamation)

$G_{\mathfrak{p}} = \langle G_{\mathfrak{p}}^{+}, \iota^0 \rangle$

$\exists\, \iota^0 \in \mathrm{Aut}(L/k_{\mathfrak{p}})$ s.t. $\iota^0|_{K^0}$: the involution induced by the conjugation $K \rightleftarrows K'$, $(\iota^0)^2 \in V^0$.

(3) Let v_L^0 be any extension of the valuation v^0 of K^0 (corresponding to Π) to a valuation of L. Then:

<u>Proposition IV-5</u> (a) There exists $\sigma \in G_{\mathfrak{p}}$ s.t.

(i) $(v_L^0)^{\sigma} = v_L^0$

(ii) σ induces mod v_L^0 the q-th power map of the residue field of L

(iii) $\sigma|_K = \iota^0|_K$ (just K, not K^0 (!))

(b) σ induces a q-th Frobenius map $\sigma_{K^\wedge}$ of the v-adic ($= v_L^0$-adic) completion $K^\wedge$ of K.

(4) Now if $k_{\mathfrak{p}}'$ denotes the algebraic closure of $k_{\mathfrak{p}}$ in L, then $L/k_{\mathfrak{p}}'$ is a 1-dim. ext'n satisfying $(L0)_{k_{\mathfrak{p}}'} \sim (L3)_{k_{\mathfrak{p}}'}$ (IV-2); hence there exists a unique $\mathrm{Aut}(L/k_{\mathfrak{p}})$-invariant S-operator S^{inv}. (Th IV-2 and the remark below). It is in particular σ-invariant. By passage to the v_L^0-adic completion, it gives a $\sigma_{K^\wedge}$-invariant S-operator, the unique $\sigma_{K^\wedge}$-invariant S operator on $K^\wedge$. If there is any embedding $k_{\mathfrak{p}}' \hookrightarrow \mathbb{C}$, then it corresponds to the canonical S-operator S_{can}.

(5) [Open problem]

With the terminologies in [18] §3, under the basic assumptions on $\mathfrak{X}_0$ and $\mathfrak{X}$ at the beginning of IV-5, prove that the set of all "rivers" (in the standard language now, "ends") on the tree $\mathfrak{T}$ associated with $\mathfrak{X}$ is equipped with the structure of

$$\mathbb{P}^1(k_{\mathfrak{p}})$$

and that the action of $\mathrm{Aut}(L/k_{\mathfrak{p}})$ on this gives rise to:

$$G_{\mathfrak{p}} \overset{?}{\twoheadrightarrow} PGL_2(k_{\mathfrak{p}}), \quad G_{\mathfrak{p}}^+ \overset{?}{\simeq} PGL_2^+(k_{\mathfrak{p}}).$$

[Truncated or "local" versions]

(6) [mod $\mathfrak{p}^{n+1}$ lifting] For $R_n = \mathcal{O}_{\mathfrak{p}}/\pi^{n+1}$ and a symmetric lifting $\mathfrak{X}_n$ over R_n of $\mathfrak{X}_0$ ([17][20]) one finds parallel objects. Here, instead of the complete "$\mathfrak{p}$-adic" field $K^{\wedge}$ we consider

$\mathfrak{K}_n$: an R_n-flat local algebra with the max. ideal (π) and the residue field $\mathbb{K}$.

A q-th Frobenius σ_n of $\mathfrak{K}_n$ determines $\omega_{n-\nu} \in D(\tilde{\mathfrak{K}}_{n-\nu})$ as its associated differential.

(7) [local mod $\mathfrak{p}^{n+1}$ lifting] Let $\mathcal{P} = \{P \leftarrow P^0 \rightarrow P'\}$ be a system of closed points of $\mathfrak{X}_0$, $\mathfrak{X}_0^{\mathcal{P}}$ be an affine open neighborhood of $\mathcal{P}$ in $\mathfrak{X}_0$, $\mathfrak{X}_n^{\mathcal{P}}$ be a (symmetric) lifting of $\mathfrak{X}_0^{\mathcal{P}}$ over R_n. For this case, a q-th Frobenius $\sigma_{\underline{P},n}$ and its associated differential $\omega_{\underline{P},n-\nu}$ can be defined, in $\mathfrak{K}_{\underline{P},n}$, $D(\tilde{\mathfrak{K}}_{\underline{P},n-\nu})$, respectively, where:

$\mathfrak{K}_{\underline{P},n}$: an R_n-flat local algebra with the max. ideal (π) and the residue field $\mathbb{K}_{\underline{P}}$, the $\underline{P}$-adic completion of $\mathbb{K}$.
($\simeq$ the field of Laurent series, 1-variable over $k_{\underline{P}}$)
$k_{\underline{P}}$: the residue field

In Ch VI, we shall need both (6)(7).

IV-6 The comparison theorem

Theorem IV-6 If a bridge $\mathcal{X}/_{\mathcal{O}}$ exists, $\mathcal{O} \overset{\iota_{\mathbb{C}}}{\hookrightarrow} \mathbb{C}$, $\mathcal{O} \underset{\iota_{\mathfrak{p}}}{\hookrightarrow} \mathcal{O}_{\mathfrak{p}}$,
domain

s.t. $\mathcal{X}_{\mathfrak{p}} = \mathcal{X} \otimes \mathcal{O}_{\mathfrak{p}}$ is as in IV-5, then

$$\underset{\text{w.r.t. } \iota_{\mathbb{C}}}{S_{can}} = \underset{\text{w.r.t. } \iota_{\mathfrak{p}}}{\mathfrak{S}}$$

on the function field of $X/_{\mathcal{O}}$.

($\because$) Characterizations Th. IV-2, IV-3, and IV-5 (3)(4) //

Thus, the canonical S-operator is "$k_{\mathfrak{p}}$-rational", "$\mathfrak{p}$-integral", and the associated differential ω is the $\mathfrak{p}$-adic solution of the differential equation

$$S_{can}\langle\omega\rangle = 0.$$

In particular, as for $S_{can,0} = S_{can} \pmod{\mathfrak{p}}$,

Corollary $S_{can,0}$ is inner w.r.t. ω_0.

When $q = p = \pi$, this together with $\gamma(\omega_0) = \omega_0$ characterizes ω_0 uniquely up to $\mathbb{F}_p^{\times}$-multiples. (cf. [14])

IV-7 Where does ω live? (notations as in IV-5)

Problems (i) Prove, modify, or disprove:

$$K^\wedge(\omega) = \text{the max. unram. ext'n of } K^\wedge \text{ in } L^\wedge \cdot k_\mathfrak{p}^{(\pi)}.$$

($L^\wedge$: the v_L^0-adic completion of L.
$k_\mathfrak{p}^{(\pi)}$: the tot. ramif. abelian ext'n $/k_\mathfrak{p}$ with the norm group $\pi^{\mathbb{Z}}$)

(ii) When $\mathfrak{X}$ arises from the $\mathfrak{p}$-canonical model of a Shimura curve (cf [18] §6), then $\hat{G}_\mathfrak{p} = GL_2(k_\mathfrak{p})/_{\pm\pi^{\mathbb{Z}}}$ acts faithfully on $L\cdot k_\mathfrak{p}^{(\pi)}$, and the action of $g \in GL_2(k_\mathfrak{p})$ on the constant field $k_\mathfrak{p}^{(\pi)}$ is via (local reciprocity)(det g^{-1}). Verify, modify, or disprove:

<Up to conjugations in $GL_2(k_\mathfrak{p})$>

★ $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k_\mathfrak{p})$ leaves the valuation $v_{0,L}$ fixed $\longleftrightarrow c = 0$

★ $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ acts on the residue field of $L\cdot k_\mathfrak{p}^{(\pi)}$ as:
$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ acts trivially, $\begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}$: the q-th power map,

action of the decompos. group on v_L^0-unram. ext'ns, in view of Problem (i)

★ $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$, $a, d \in \mathcal{O}_\mathfrak{p}^\times$ acts on ω, as $\omega \longrightarrow a^2\omega$.

These are certainly known in the elliptic modular case. In V-2, we shall use this to construct t_n's s.t. $\omega \equiv d\log t_n \mod p^{n+1}$ inside $L^\wedge \cdot k_\mathfrak{p}^{(\pi)}$, which also answers Problem (i) in this case.

V The dlog form of ω_n when $q = p = \pi$ (Three aspects)

V-1 [Basic, formal] Let k: a finite field, char. p,

$\mathbb{K}$: either a function field of 1-var$/k$,

or the field of power series in 1-var$/k$.

$W(k)$: the ring of Witt vectors, $R_n = W(k)/p^{n+1}$ $(n \geq 0)$.

$\mathfrak{K}_n$: an R_n-flat local algebra with max. ideal (p), residue field $\mathfrak{K}_0 = \mathbb{K}$.[1]

$\tilde{\mathfrak{K}}_n = \bigcup$ (fin. etale ext'ns of $\mathfrak{K}_n$); $\tilde{\mathfrak{K}}_0 = \mathbb{K}^{sep}$: the separable closure.

$\sigma_n : \mathfrak{K}_n \to \mathfrak{K}_n$: a p-th Frobenius (map), i.e., an endomorphism inducing the p-th power morphism of $\mathfrak{K}_0 = \mathbb{K}$. Its unique extension $\tilde{\sigma}_n : \tilde{\mathfrak{K}}_n \to \tilde{\mathfrak{K}}_n$ as a p-th Frobenius of $\tilde{\mathfrak{K}}_n$ will be abbreviated as σ_n.

The "σ_n-associated differential" is w.r.t. $\pi = p$.

Theorem V-1 For each given p-th Frobenius $\sigma_n : \mathfrak{K}_n \to \mathfrak{K}_n$ $(n \geq 1)$, there exists $t_n \in \tilde{\mathfrak{K}}_n$ with $t_0 \notin (\mathbb{K}^{sep})^p$, s.t.

$$t_n^{\sigma_n} = t_n^p .$$

Accordingly, the differential associated with σ_n is given by

$$\omega_{n-1} = d \log t_{n-1} .$$

(2) For $t_n' \in \tilde{\mathfrak{K}}_n$ with $t_0' \notin (\mathbb{K}^{sep})^p$,

$$t_n'^{\sigma_n} = t_n'^p \iff t_n' = t_n^r u^{p^n} \quad \left(\begin{matrix} \exists r \in \mathbb{Z}, \not\equiv 0 \pmod p \\ \exists u \in \tilde{\mathfrak{K}}_n^\times \end{matrix} \right)$$

---

1) Here and in the following, the same symbol with different suffixes n indicates that the objects are projection-compatible. We shall sometimes say "t_n is above t_{n-1}", etc.

This was stated in [17] (§9 Th 3) as a remark without proof. Here it is more relevant. The case $n=1$ is a direct consequence of Prop IV-4. (Since $\gamma(\omega_0)=\omega_0$, $\omega_0 = d\log^{\exists} t_0$; take any t_1 above t_0 and put $t_1^{\sigma_1} = t_1^p + ps_0$. Then the equality $\omega_0 = d\log t_0$ gives $ds_0 = 0$; hence $s_0^{1/p} \in \mathbb{K}^{sep}$; and $t_1' = t_1 - ps_0^{1/p}$ satisfies $t_1'^{\sigma_1} = t_1'^p$; the second assertion (2) for $n=1$ is by the uniqueness of ω_0 up to $(\mathbb{Z}/p)^\times$-multiples.). The rest is by induction on $n \geq 1$ and the following lemma, which is what we really need in Ch. VI, constitutes each induction step.

<u>Lemma V-1</u>[1] Let $\sigma_n : \mathfrak{K}_n \to \mathfrak{K}_n$ $(n \geq 1)$ be a p-th Frobenius. Suppose $\exists\, t_n \in \hat{\mathfrak{K}}_n$, $t_0 \notin \hat{\mathfrak{K}}_0^p$ s.t. $t_n^{\sigma_n} = t_n^p$. Let $\sigma_{n+1} : \mathfrak{K}_{n+1} \to \mathfrak{K}_{n+1}$ be any lifting of σ_n as a Frobenius. For any auxiliary choice of $t_{n+1} \in \tilde{\mathfrak{K}}_{n+1}$ which lifts t_n, set

$$t_{n+1}^{\sigma_{n+1}} = t_{n+1}^p + p^{n+1} s_0 \qquad (s_0 \in \mathbb{K}^{sep}),$$

$$\xi_0 = -t_0^{-p} ds_0, \quad a_0 = \frac{\xi_0}{\omega_0}, \quad \wp(f_0) = a_0$$

$(\omega_0 = d\log t_0,\ \xi_0 \in D(\mathbb{K}^{sep}),\ a_0, f_0 \in \mathbb{K}^{sep};\ \wp(*) = *^p - *)$.

We shall call s_0: <u>the σ_{n+1}-remainder</u> <u>w.r.t.</u> t_{n+1}.

---

1) For $p=2$, a slight modification may be necessary. So for safety we assume here that $p > 2$.

Then: (0) ξ_0 and hence also a_0 and $f_0 + \mathbb{F}_p$ are independent of the choice of t_{n+1}. Denote them as $a_0 := a_0(\sigma_{n+1}, t_n)$, etc.

(1) For any $v_n \in \tilde{\mathcal{O}}_n$, $v_0 \neq 0$,

$$\underbrace{a_0(\sigma_{n+1}, t_n v_n^{p^n})}_{\Vert\downarrow \text{ abbrev. } a_0'} - \underbrace{a_0(\sigma_{n+1}, t_n)}_{\Vert\downarrow\ a_0} = -\wp\left(\frac{d\log v_0}{\omega_0}\right).$$

(2)
$$f_0\omega_0 = d\log u_0 \qquad (\exists u_0 \in \mathbb{K}^\times).$$

(3) If we choose v_n s.t. $v_0 = u_0$, then

$$a_0(\sigma_{n+1}, t_n v_n^{p^n}) = 0;$$

hence the σ_{n+1}-remainder w.r.t. $t_{n+1} v_{n+1}^{p^n}$ (above v_n) is a p-th power and hence $\exists_1\ t'_{n+1} \equiv t_n v_{n+1}^{p^n} \mod p^{n+2}$ s.t.

$$t'^{\sigma_{n+1}}_{n+1} = t'^{p}_{n+1}.$$

(4) The σ_{n+1}-assoc. diff. ω_n can be expressed, in terms of the initially given t_n, as

$$\omega_n = (d\log t_n)(1 + p^n f_0)$$

up to $R_n^\times$-multiples. ($f_0 = f_0(\sigma_{n+1}, t_n)$).

(end of Lemma V-1)

(Proof) (0) Obvious.

(1) Set $v_1^{\sigma_1} = v_1^p + p r_0$. Then by direct computations,[1)]

$$a_0' - a_0 = -v_0^{-p} dr_0/\omega_0 .$$

But from the definition of ω_0 using the above $v_1^{\sigma_1}$-expression and by comparing with the identity $\omega_0 = d\log t_0$ we obtain

$$v_0^{-p} dr_0/\omega_0 = \wp\left(\frac{d\log v_0}{\omega_0}\right)$$

(2) Let γ be the Cartier operator on $D(\mathbb{K}^{sep})$. Then

$$\left\{\begin{aligned} f_0^p - f_0 &= a_0 \\ \xi_0 &= -t^{-p} ds_0 \\ \omega_0 &= t_0^{-1} dt_0 \end{aligned}\right\} \Rightarrow \left\{\begin{aligned} f_0^p\omega_0 - f_0\omega_0 &= \xi_0 \\ \gamma(\xi_0) &= 0 \\ \gamma(\omega_0) &= \omega_0 \end{aligned}\right\} \Rightarrow \gamma(f_0\omega_0) = f_0\omega_0 .$$

(3) Since $a_0 = \wp(f_0)$ by definition, (1) and (2) give $a_0' = 0$, for $v_0 = u_0$.

(4)
$$\begin{aligned} \omega_n \equiv d\log t_{n+1}' &\equiv d\log t_{n+1} + p^n \overbrace{d\log u_0}^{f_0\omega_0} \\ &= (d\log t_n)(1 + p^n f_0) \end{aligned}$$

//

1) For $p=2$, a slight modification is necessary

V-2 Construction of $\omega_{n-1} = d\log t_n$ in the elliptic modular case

When Γ is any congruence subgroup of $PSL_2(\mathbb{Z}[\frac{1}{p}])$ and $\pi = p$, we have $Lk_\pi = L(\mu_{p^\infty})$ on which $GL_2(\mathbb{Q}_p)/\pm\langle p^{\mathbb{Z}}\rangle$ acts faithfully from the right.

[Partial Galois Picture] (cf. IV-7).

$\left(\begin{array}{l} g \in GL_2(\mathbb{Z}_p)/_{\pm 1} \text{ acts on} \\ \mu_{p^\infty} \text{ by } \zeta \to \zeta^{\det(g)} \end{array} \right)$

$\sigma = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$

$$\begin{tikzcd}[column sep=small]
 & & L(\mu_{p^\infty}) \arrow[d, dash] & \\
\left\{\begin{pmatrix} 1 & p^{-n}b \\ 0 & 1 \end{pmatrix}\right\} \arrow[r, leftrightarrow] & M^{\sigma^n} \arrow[r, dash, "p^n\text{-cyclic Kummer}"] \arrow[d, dash] & M \arrow[r, leftrightarrow] \arrow[d, dash] & \left\{\tau^b = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right\} \arrow[d, dash] \\
\left\{\begin{pmatrix} 1 & p^{-n}b \\ 0 & d \end{pmatrix}\right\} \arrow[r, leftrightarrow] & M_1^{\sigma^n} \arrow[r, dash] & M_1 \arrow[r, leftrightarrow] \arrow[d, dash] & \left\{\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}\right\} : \text{inertia group}/K \text{ wrt } v_L^0 \arrow[d, dash] \\
 & & M_0 \arrow[r, leftrightarrow] \arrow[d, dash] & \left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right\} : \text{decomposition group}/K \text{ wrt } v_L^0 \arrow[d, dash] \\
 & & K \arrow[r, leftrightarrow] & \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}_p)/_{\pm 1}\right\}
\end{tikzcd}$$

We shall show:

" t_n <u>can be found among Kummer generators of</u> M/M^{σ^n} "

To begin with, basic remarks; • $\tau = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\sigma\tau\sigma^{-1} = \tau^p$,

- For $\tau_n := \sigma^{-n}\tau\sigma^n = \tau^{p^{-n}}$, $\quad Gal(M/M^{\sigma^n}) = \langle \tau_n \rangle \quad (n \geq 1)$.

- By completion $\hat{}$, $\begin{cases} \hat{K} = \hat{M_0} & \text{but all other parts remain "parallel"} \\ \sigma : \text{a } p\text{-th Frobenius of } L(\mu_{p^\infty})^{\wedge}. \end{cases}$

[Claims, to be proved in order] $\mu_{p^n} = \langle \zeta_n \rangle$, $\zeta_{n+1}^p = \zeta_n$

(A) $\exists\, t_n \in M_1^\times$, s.t. $\mathrm{ord}_p(t_n) = 0$, $t_n^{\tau_n} = \zeta_n t_n$.

(B) Such t_n satisfies $\mathrm{ord}_p(dt_n) = 0$.

(C) $r_n = t_n^\sigma / t_n^p$ satisfies $r_n \in M_1^{\sigma^n}$, $\mathrm{ord}_p(r_n - 1) \geq 1$.

(D) $$(d\log t_n)^\sigma \equiv p\,(d\log t_n) \bmod p^{n+1} \quad (\text{w.r.t. } v_L^0);$$

hence $\omega_{n-1} \equiv d\log t_n \pmod{p^n}$ is the σ-assoc. differential.

We may choose ω_n $(n \geq 0)$ compatibly.

(E) $$\omega_{n-1}^{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)} = a^2\,\omega_{n-1} \qquad (\forall a, d \in \mathbb{Z}_p^\times,\ b \in \mathbb{Z}_p);$$

hence $$\mathrm{Gal}\left(\mathbb{K}(\omega_{n-1})/\mathbb{K}\right) \simeq \mathbb{Z}_p^\times / \{a\,;\ a^2 \equiv 1\ (p^n)\}$$
$$(\simeq \mathbb{Z}_p^\times / (\pm 1 + p^n \mathbb{Z}_p) \quad \text{if } p > 2.)$$

[Proofs] [1].

(A) M/M^{σ^n} being p^n-cyclic, Kummer, $\exists\, t_n \in M^\times$ s.t. $t_n^{\tau_n} = \zeta_n t_n$.

Then t_n^δ for $\delta = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ also satisfies this, because $\tau_n \delta = \delta\, \tau_n^d$.

Hence one may replace t_n by $\mathrm{tr}_{/M_1}(\xi t_n)$ for $\xi \in \mu_{p^\infty}$.

For some ξ this is $\neq 0$; hence $\exists\, t_n \in M_1^\times$ s.t. $t_n^{\tau_n} = \zeta_n t_n$.

Since M_1/K is unramified, we may multiply some power of p and assume $\mathrm{ord}_p(t_n) = 0$.

---

1) These are so elementary, pretty and unsophisticated, that I could not help writing up the key points.

(B) $\quad M_1 = M_1^{\sigma^n}(t_n), \quad t_n^{p^n} \in M^{\sigma^n} \cap M_1 = M_1^{\sigma^n}$; (ord$_p = 0$)

hence $\quad M_1 = M_1^{\sigma}(t_n), \quad t_n^{p} \in M^{\sigma} \cap M_1 = M_1^{\sigma}$.

Suppose, on the contrary, that $d\bar{t}_n = 0$. Then one may replace t_n by $u^p t_n$ for some unit u and assume $\bar{t}_n = 1$. But the adjunction of one p-th root of an elt $\equiv 1 \pmod p$ of M_1^{σ} would yield, after completion, either the trivial ext'n, or a totally ramified ext'n of degree p, thus cannot yield M_1. (For $p=2$, we need $n \geq 2$ and use $M_1/M_1^{\sigma^2}$.)

(C, D) By $\sigma \tau_n \sigma^{-1} = \tau_n^p$, we see that both t_n^{σ} and t_n^p are multiplied by ζ_{n-1} by the action of τ_n; hence $\Upsilon_n^{\tau_n} = \Upsilon_n$; hence $\Upsilon_n \in M^{\sigma^n} \cap M_1 = M_1^{\sigma^n}$. Moreover, $\Upsilon_n \equiv 1 \pmod p$;

$\Upsilon_n = 1 + p S_n^{\sigma^n}$; S_n: integral $\in M$. Since $\mathrm{ord}_p(dS_n^{\sigma_n}) = \mathrm{ord}_p(dS_n) + n$, we obtain $d\Upsilon_n \equiv 0 \pmod{p^{n+1}}$; whence (D). (The last point is obvious.)

(E) Put $[a] = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. From $t_n^{\tau_n} = \zeta_n t_n$, and $\zeta_n^{[a]} = \zeta_n^{a^2}$,

$\Rightarrow \quad t_n^{[a]\tau_n} = \zeta_n^{a^2} t_n^{[a]}, \quad t_n^{\tau_n \langle a^2 \rangle} = \zeta_n^{a^2} t_n^{\langle a^2 \rangle}$, where $\langle a^2 \rangle \in \mathbb{Z}$, $\equiv a^2 \pmod{p^n}$. Hence $t_n^{[a]} / t_n^{\langle a^2 \rangle}$: τ_n-inv.

$\therefore \in M^{\sigma^n}$, integral. Therefore, $d\log\left(t_n^{[a]} / t_n^{\langle a^2 \rangle}\right) \equiv 0 \pmod{p^n}$;

hence $\omega_{n-1}^{[a]} = a^2 \omega_{n-1}$. Since $\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \in$ Inertia, (E) follows. //

By taking limit in the completion we obtain $\omega = \lim_{n} \omega_{n-1}$ $\in D(\hat{M_1})$, and (E) gives

$$K^{\wedge}(\omega) = \hat{M_1} \quad (= \text{the max. unram. subext'n of } K^{\wedge} \text{ in } \hat{L}(\mu_{p^\infty})),$$

which settles Problem (i) of IV-7 in this case,

Together with

$$\chi\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right) = \chi\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right) = a^2 \quad (a \in \mathbb{Z}_p^\times);$$

This induces

$$\chi : Gal(\hat{M_1}/\hat{K}) \xrightarrow{\sim} (\mathbb{Z}_p^\times)^2.$$

In this elliptic modular case, ω has other well-known interpretations (Tate's q; Dwork's p-adic $d\tau$) from the moduli aspects. The above construction[1] is algebraic, and is based only on the Galois picture described above, so it would also be applicable to the case of Shimura curves (for $k_\mathfrak{z} = \mathbb{Q}_p$) where there are no cusps and where the moduli interpretation is more complicated.

---

1) It was noticed during my stay at Stanford (1970~71) and was communicated to some senior colleagues but remained in my file unpublished. Too small to insist on something but too pretty not to be mentioned...

V-3 The invariant S-operator in the elliptic modular case.

Coming back to the λ-line $X = \mathbb{P}^1 - \{0,1,\infty\}$ in II-5; since Δ is a triangular group, the formula for S_{can} is known (cf. e.g. [13] §2.4);

[Over $\mathbb{C}$] $\quad S_{can}\langle\eta\rangle = \langle\eta, d\lambda\rangle - \dfrac{\lambda^2-\lambda+1}{\lambda^2(1-\lambda)^2}(d\lambda)^{\otimes 2}$.

By the comparison theorem, (IV-6),

[p-adic] $\quad \mathbb{S}\langle\eta\rangle =$ the same as above $= S_\omega\langle\eta\rangle$.

In this case, $L(\mu_{p^\infty}) = \mathbb{Q}_p(\lambda,$ the x-coordinates of p-power div. pts of $E_\lambda)$

If we denote simply by $\mathbb{K}(\omega_n)$ the residue field of $\hat{K}(\omega_n)$, the tower $\{\mathbb{K}(\omega_n)/\mathbb{K}\}_{n\geq 0}$ of $(\mathbb{Z}_p^\times/\pm 1 (\mathrm{mod}\ p^n))$-ext'ns over $\mathbb{K} = \mathbb{F}_p(\lambda)$ is the same as the tower studied in Igusa [Ig 3]. There, he computed wild ramifications in order to compute the genus of each layer of the tower. From his results on ramifications we obtain easily:

<u>Corollary of [Ig 3]</u> : Let $\mathbb{K}(\omega_n)^{(p)}$ denote the cyclic subextension of degree p^n in $\mathbb{K}(\omega_n)$. Then, above each supersingular λ_0, the conductor exponent of $\mathbb{K}(\omega_n)^{(p)}/\mathbb{K}$ is

$$f_n(p) = p^n + 2(p^{n-1} + \cdots + 1).$$

<u>Conjecture</u> Whenever $q = p (= \pi)$, the same formula holds.

The affirmative answer for $n = 1$ is obtained in the next § VI, in connection with the problem of lifting of $\mathfrak{X}_0$ over $\mathbb{Z}/p^3$.

[Over $\mathbb{F}_p$] The S-operator S_p defined by the same formula as above over $\mathbb{F}_p$ is <u>inner</u> over $\mathbb{K}(\omega_0)$; $S_p = S_{\omega_0}$. The differential ω_0 lives in a cyclic $\frac{1}{2}(p-1)$ fold cover of $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$, defined by

$$\omega_0^{\otimes(p-1)} = \frac{f(\lambda)^2}{(\lambda(1-\lambda))^{p-1}} (d\lambda)^{\otimes(p-1)}.$$

It can be characterized by two equations

$$S_p\langle\omega_0\rangle = 0, \qquad \gamma(\omega_0) = \omega_0. \qquad ([4]\ \mathrm{Th}\ 4).$$

VI The lifting problem

VI-1 Let $\mathbb{X}$: a proper smooth $\mathbb{F}_q$-irreducible curve,

$\phi \neq \mathfrak{S} \subseteq \mathbb{X}(\mathbb{F}_{q^2})$ ($\mathfrak{S} \neq \phi$ implies the exact constant field is $\mathbb{F}_q$ or $\mathbb{F}_{q^2}$; in the former case assume $\mathfrak{S}$: stable under conjug/$\mathbb{F}_q$)

$\mathfrak{X}_0 = \{ \mathbb{X} \leftarrow \mathbb{X}^0 \rightarrow \mathbb{X}' \}$; $\mathbb{X}^0 = \mathbb{X}^0_{\mathfrak{S}}$ (see III-2)

R : a complete discrete valuation ring s.t. $R/\pi = \mathbb{F}_q$.
π : a prime element

$R_n = R/\pi^{n+1}$ $(n \geq 0)$.

In [17] [20], we started our study of liftings $\mathfrak{X}_n = \{ X_n \leftarrow X^0_n \rightarrow X'_n \}$ (resp. $\mathfrak{X} = \{ X \leftarrow X^0 \rightarrow X' \}$) of $\mathfrak{X}_0$ to system(s) of proper flat R_n (resp. R)-schemes by cohomological method. ($X_{(n)}, X'_{(n)}$: smooth, X^0 : normal). $\mathfrak{X}$ corresponds bijectively with compatible $\{\mathfrak{X}_n\}_{n \geq 0}$.

Results in [17] contain :

(A) Association of a pair $(\omega_{n-1}, \omega'_{n-1})$ of differentials to each $(\mathfrak{X}_n, {}^t\mathfrak{X}_n)$; traspose

(B) Establishment of the "local-global principle" using (A) (in this formulation, just when $q = p$) (see VI-2 below)

(C) Application of (B) to the first infinitesimal step $(n=0 \rightarrow n=1)$ (see VI-3 below).

Here, we shall further assume

(#) $\quad q = p, \quad |\mathfrak{G}| = (p-1)(g_{*}-1); \quad R = \mathbb{Z}_p.$

This assumption on $|\mathfrak{G}|$ is natural (Ch □). We add here that this is an <u>extreme</u> case. The existence of a lifting of $\mathfrak{X}_0$ to an object in char. 0 can be expected <u>only</u> when $|\mathfrak{G}| \geq (p-1)(g_{*}-1)$. [1]

Moreover,

<u>Theorem VI-1 ([20] Th4)</u>[2] When $|\mathfrak{G}| = (p-1)(g_{*}-1)$ and $n \geq 1$, there exists <u>at</u> <u>most</u> <u>one</u> lifting $\mathfrak{X}_n$ of $\mathfrak{X}_0$ over R_n. It is necessarily <u>symmetric</u>. (i.e., ${}^t\mathfrak{X}_n$ "=" $\mathfrak{X}_n$).

By this, considering a pair $(\omega_{n-1}, \omega'_{n-1})$ as in [17] is equivalent to considering a single differential ω_{n-1} satisfying a certain symmetricity condition, associated to $\mathfrak{X}_n$ as in Ch IV.

A criterim for the existence of the lifting <u>over</u> $R = \mathbb{Z}_p$, together with some examples were also given in [20] (Th. 3, Examples 2, 3).

---

1) cf. either [18] §1, or [20] §1 (Cor 1 of Th 2).

2) To be precise, what is stated in Th 4 is the uniqueness of $\mathfrak{X}/R$, but the proof in §2.6 gives a stronger statement, that each infinitesimal lifting $\mathfrak{X}_{n+1}/\mathfrak{X}_n$ is unique (because the key point lies on Ker $F = 0$, derived from the uniqueness of the first-step lifting) Cf. Cor 1, 2 of Th VI-3 below.

As for the assumption $R = \mathbb{Z}_p$, it is too restrictive from the point of view of lifting an object over $\mathbb{F}_p$ to that in char. 0; the first lift may be over $\mathbb{F}_p[\varepsilon]$ $(\varepsilon^2=0)$ (in which case ω_0 is <u>exact</u> instead of log-exact) but finally over, say, $\mathbb{Z}_p[\sqrt{p}\,]$. In [17][20], these cases are included.[1] But here, we must rely on the <u>log</u>-exactness of ω_n at each step, and so we restrict ourselves to liftings over $\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p$. Now, for $R = \mathbb{Z}_p$, we ask the following "fatal ?" questions.[2]

Put $n_{(\mathscr{X},\mathfrak{S})} := \operatorname{Sup}\{n;\ \exists\, \mathfrak{X}_n \text{ that lifts } \mathfrak{X}_0\}$

$(= +\infty \iff \exists\, \mathfrak{X}$ that lifts $\mathfrak{X}_0)$

<u>(Q VI-1)</u> (i) Does there exist a uniform bound $N_0 < \infty$ s.t.

$$n_{(\mathscr{X},\mathfrak{S})} \geq N_0 \quad \text{implies} \quad n_{(\mathscr{X},\mathfrak{S})} = \infty \quad ?$$

(i)′ $N_0 = 2$? (i.e., $\exists\, \mathfrak{X}_2 \Longrightarrow \exists\, \mathfrak{X}$?) (too optimistic ?)

(ii) If not, is there a simple upper bound for <u>finite</u> $n_{(\mathscr{X},\mathfrak{S})}$, in terms of p, $g_{\mathscr{X}}$, or the p-rank of $\mathscr{X}$ (modified w.r.t. $\mathfrak{S}$) ?

We give an example in VI-8 of $(\mathscr{X},\mathfrak{S})$ s.t. $n_{(\mathscr{X},\mathfrak{S})} = 1$ (i.e., $\exists\, \mathfrak{X}_1$ but $\nexists\, \mathfrak{X}_2$), which gives $N_0 > 1$ (if exists at all).

---

1) e.g. Th 5 in [17] for "Case 2", the invariants m, r of $(\mathscr{X},\mathfrak{S})$, etc. in [20].

2) At present, only to keep these "as central questions" in mind.

VI-2 Now let us recall the local-global principle ([17] Th 4).

Theorem VI-2 Suppose $\mathcal{X}_\pi$ is a symmetric lifting of $\mathcal{X}_0$ over $R_n = \mathbb{Z}/p^{n+1}$, and ω_{n-1} mod p^n is the associated differential (w.r.t. $\pi = p$).

Then

$$\begin{array}{ccccl} \mathcal{X}_{n+1} & \longleftrightarrow & \omega_n & \text{s.t.} & (*) \\ (\text{liftings of } \mathcal{X}_n) & & (\text{liftings of } \omega_{n-1}) & & \\ \text{up to} \simeq & & & & \end{array}$$

(*) at each system of closed pts $\mathfrak{P} = \{P \leftarrow P^0 \rightarrow P'\}$ of $\mathcal{X}_0$, $\exists$ a local lifting $\mathcal{X}_{n+1}^{\mathfrak{P}}$ of $\mathcal{X}_n$ in an affine nbd of $\mathfrak{P}$, symmetric if ${}^t\mathfrak{P} = \mathfrak{P}$, whose assoc. differential $\omega_{\mathfrak{P}, n-1}$ "coincides" with ω_n.

Rmk 1 Local liftings always exist. Unique if $P \notin \mathfrak{S}$, and when $P \in \mathfrak{S}$, such liftings (mod $\simeq$) form a principal homog. space of $\mathfrak{k}_P$ ([17] §5).

Rmk 2 If $\mathfrak{K}_n$ denotes the local ring of X_n at the generic point, which is a flat local R_n-algebra with max. ideal (p) and the residue field $\mathfrak{K}_0 = \mathbb{K} = \mathbb{F}_q(\mathscr{X})$, then ω_{n-1} lives in $D(\tilde{\mathfrak{K}}_{n-1})$. At each closed point P of $\mathscr{X}$, if $\mathfrak{K}_{P,n}$ denotes the flat local R_n-algebra with max. ideal (p) whose residue field $\mathfrak{K}_{P,0}$ is the completion $\mathbb{K}_P$ of $\mathbb{K}$ at P, which is derived from the local ring of X_n at $\mathbf{P}$ by standard processes, then $\omega_{P,n-1}$ lives in $D(\tilde{\mathfrak{K}}_{P,n-1})$. "Coincides" means "corresponds via canonical maps".

VI-3 Liftings to over $R_1 = \mathbb{Z}/_{p^2}$. (a special case of [17] Th 5)

Theorem VI-3 Let $|\mathfrak{S}| = (p-1)(g-1)$, $\mathbb{K}$: the function field of $\mathfrak{X}$.

Then
$$\underset{(\text{up to } \simeq)}{\mathfrak{X}_1/\mathfrak{X}_0} \quad \underset{1:1}{\longleftrightarrow} \quad \omega_0^{\otimes(p-1)} \in D^{p-1}(\mathbb{K}) \text{ satisfying:}$$

$$\begin{cases} \text{(A)} & (\omega_0^{\otimes(p-1)}) = 2\mathfrak{S}; \\ \text{(B)} & \gamma(\omega_0) = \omega_0 \quad \text{the Cartier operator} \\ \text{(C)} & \text{symmetricity above } \mathfrak{S}\text{; i.e., for each } P \in \mathfrak{S}, \end{cases}$$

$$\varepsilon_0 := \left(\frac{\omega_0^{\otimes(p-1)}}{x_P^2 (dx_P)^{\otimes(p-1)}} \right)^{-1}_{P} \in \mathbb{F}_p^\times$$

local parameter   value at P

($\varepsilon_0 \pmod{\mathbb{F}_p^{\times}}$ is indep of the choice of x_P;
in fact, $\varepsilon_0 \bmod (k_P^{\times p+1})$ is.)

Cor 1 $\exists\, \mathfrak{X}_1 \rightarrow \exists_1\, \mathfrak{X}_1$

Cor 2 Given $\mathfrak{X}_n/\mathfrak{X}_0$, $(n \geq 1)$ $\exists\, \mathfrak{X}_{n+1}/\mathfrak{X}_n \rightarrow \exists_1$

$(\because)$ $\exists\, \mathfrak{X}_n \longrightarrow \exists\, \mathfrak{X}_1 \longrightarrow \exists_1\, \mathfrak{X}_1 \longrightarrow m = 0$ (cf. [20]))

Remark 1 As for (A), from just local reasons it comes out only as $(\omega_0^{\otimes(p-1)}) \leq 2\mathfrak{S}$. The "$=$" follows because $|\mathfrak{S}| = (p-1)(g-1)$.

We shall often write $\mathbb{K}^* = \mathbb{K}(\omega_0)$. For $p=2$, $\mathbb{K}^* = \mathbb{K}$.

<u>Proposition VI-3</u> Suppose $\omega_0^{\otimes(p-1)} \in D^{p-1}(\mathbb{K})$ satisfies (A)(B)(C), and let $p>2$. Let $P \in \mathfrak{S}$, and P^*: a point (place) of $\mathbb{K}^*$ above P. Then (i) $\kappa_{P^*} = \kappa_P(\sqrt{\varepsilon_0})$ for the residue fields,

(ii) $e_{P^*/P} = \frac{1}{2}(p-1)$ for the ramification index,

(iii) $\operatorname{ord}_{P^*}(\omega_0) = \frac{1}{2}(p-1)$.

(∵) $\underbrace{\mathbb{K}_P(\omega_0)}_{\text{the completion}} = \mathbb{K}_P((\varepsilon_0^{-1} x_P^2)^{\frac{1}{p-1}}) \supseteq \mathbb{K}_P(\sqrt{\varepsilon_0})$ gives (i)(ii).

(iii) Since $e = e_{P^*/P} \not\equiv 0 \pmod p$,

$$\operatorname{ord}_{P^*}(\eta) + h = e\cdot(\operatorname{ord}_P(\eta) + h) \qquad (\eta \in D^h(\mathbb{K}^*))$$

For $\eta = \omega_0^{\otimes(p-1)}$, RHS $= \frac{1}{2}(p-1)(p+1) =$ LHS $= (p-1)\operatorname{ord}_{P^*}\omega_0 + (p-1)$;

whence (iii) //

<u>VI-4</u> <u>Discussions</u> When $\mathfrak{X}_n$ exists, its associated differential (w.r.t. $\pi = p$) ω_{n-1} defines, as in IV-4 a character

max. abelian ext'n

$$\chi_{n-1} : \mathrm{Gal}(\mathbb{K}^{ab}/\underbrace{\mathbb{K}}_{=\mathbb{F}_q(\mathbb{X})}) \to R_{n-1}^{\times}.$$

Let (as before) $\mathbb{K}(\omega_{n-1})/\mathbb{K}$ denote the subfield corresponding to $\mathrm{Ker}(\chi_{n-1})$.

Since there is at most one lifting for a given pair $(\mathbb{X}, \mathfrak{S})$, the following questions make sense ("describe" means "in terms of $(\mathbb{X}, \mathfrak{S})$").

(Q1) Describe the composite map

$$I_{\mathbb{K}}/\mathbb{K}^{\times} \longrightarrow \mathrm{Gal}(\mathbb{K}^{ab}/\mathbb{K}) \xrightarrow{\chi_{n-1}} R_{n-1}^{\times}.$$

idèles reciprocity

(Q2) Does the existence of "admissible χ_{n-1}" mean that of "real ω_{n-1}"?

$(Q1)_{\mathfrak{p}}$ Describe

a closed pt of $\mathbb{X}$

$$\mathbb{K}_{\mathfrak{p}}^{\times} \longrightarrow \mathrm{Gal}(\mathbb{K}_{\mathfrak{p}}^{ab}/\mathbb{K}_{\mathfrak{p}}) \xrightarrow{\chi_{\mathfrak{p},n-1}} R_{n-1}^{\times}.$$

local reciprocity

$(Q2)_{\mathfrak{p}}$ Does the existence of "admissible $\chi_{\mathfrak{p},n-1}$" mean that of "real $\omega_{\mathfrak{p},n-1}$"?

But <u>how</u> can one give explicit descriptions of these local questions without having explicit presentation of each element of $\mathbb{K}_P$? Unlike $\mathbb{Q}_p$, presentation of each <u>element</u> of $\mathbb{K}_P \simeq \kappa_P((x_P))$ depends on the (a priori non-canonical) choice of a local parameter x_P. To be more specific, we will see in due course that for $P \in \mathfrak{S}$, if we call

$$\psi_{P,1} : \mathbb{K}_P^\times \to \mathbb{F}_p$$

the composite map, $(Q1)_P$ for $n=2$ followed by $R_1^\times \twoheadrightarrow \mathbb{F}_p$, $1+pa \mapsto a$ and if we put

$$U_P = \mathcal{O}_P^\times, \quad U_P^{(i)} = 1 + m_P^i \quad (i \geq 1) \quad \left(\begin{matrix}\mathcal{O}_P : \text{the val. ring,} \\ m_P : \text{the max. ideal}\end{matrix} \text{ in } \mathbb{K}_P\right),$$

then,

$$\mathcal{W} = \mathcal{W}_{\psi_{P,1}} = \mathrm{Ker}(\psi_{P,1})|_{U_P^{(1)}} \text{ has conductor exponent} = p+2 \text{; i.e.,}$$

$$(*) \qquad U_P^{(p+2)} \subseteq \mathcal{W}, \qquad U_P^{(p+1)} \not\subset \mathcal{W}.$$

But there are so many $(\sim p^p)$ open subgroups $\mathcal{W} \subset U_P^{(1)}$ with index p satisfying $(*)$. Possibly such $\mathcal{W}$'s can be transformed to each other by automorphisms of $\mathbb{K}_P$ induced by changing the uniformizer x_P.[1)]

---

1) A closely related question is: whether two abelian extensions of $\mathbb{K}_P$ with the "same" Galois and the inertia groups and the equal conductors can be transformed to each other by an extension of such an automorphism of $\mathbb{K}_P$. The answer to (correctly modified) question should have been published a "century" ago! (Please kindly let me know)

And we must describe $\mathcal{W}_{\Psi_{\mathfrak{p},1}}$ explicitly in terms of $(\mathcal{H}, \mathfrak{S})$. So, unless one can describe this just in terms of ω_0 (or $\omega_0^{\otimes(p-1)}$), which I have not succeeded, the only other way is to find $x_{\mathfrak{p}}$ with which ω_0 (or $\omega_0^{\otimes(p-1)}$) can be expressed in a reasonably simple "normal form", expecting that the restriction on $x_{\mathfrak{p}}$ by this property is sufficient for our purpose. This is what we are going to do in the next VI-5, 6.

VI-5 Local study at $\mathfrak{p} \in \mathfrak{S}$ ($\mathcal{O}_{\mathfrak{p}} = \kappa_{\mathfrak{p}}[[x]]$, $\kappa_{\mathfrak{p}} \subseteq \mathbb{F}_{p^2}$)

(1) The local versions of the conditions (A)(B)(C) for $\omega_0^{\otimes(p-1)}$ (VI-3) are:

$$(\alpha)\quad \mathrm{ord}_{\mathfrak{p}}\, \omega_0^{\otimes(p-1)} = 2, \qquad (\beta)\quad \gamma(\omega_0) = \omega_0, \qquad (\gamma)_{\varepsilon_0}:\ \underbrace{\left(\frac{\omega_0^{\otimes(p-1)}}{x^2 (dx)^{\otimes(p-1)}}\right)_{\mathfrak{p}}}_{\varepsilon_0^{-1}} \in \mathbb{F}_p^{\times}.$$

If we express $\omega_0^{\otimes(p-1)}$ as

$$\omega_0^{\otimes(p-1)} = \frac{x^2 (dx)^{\otimes(p-1)}}{g(x) + x^{p+1}} \qquad (g(x) \in \mathbb{K}_{\mathfrak{p}}),$$

then, in terms of $g(x)$, $(\alpha)(\beta)(\gamma)_{\varepsilon_0}$ are equivalent (respectively) to:

$$(\alpha')\quad g(x) \in \kappa_{\mathfrak{p}}[[x]]^{\times}, \qquad (\beta')\quad \gamma(g(x)x^{-2}dx) = 0, \qquad (\gamma')_{\varepsilon_0}:\ g(0) = \varepsilon_0 .$$

$$\Updownarrow$$

$$\mathrm{Coeff}(g(x), x^j) = 0 \quad \text{if } j \equiv 1 \pmod p$$

<u>Proposition VI-5</u> Fix $\varepsilon_0 \in \mathbb{F}_p^\times$. Then <u>any two elements</u> of $D^{p-1}(\mathbb{K}_p)$ satisfying $(\alpha)(\beta)(\gamma)_{\varepsilon_0}$ <u>can be transformed to each other</u> by a (continuous) field automorphism of $\mathbb{K}_p$ induced by changing the variable $x \to \sum_{i\geq 1} a_i x^i$ $(a_i \in k_p,\ a_1 = 1)$.

In other words, if $F(x)(dx)^{\otimes(p-1)}$, for some $F(x) \in \mathbb{K}_p$, satisfies $(\alpha)(\beta)(\gamma)_{\varepsilon_0}$, then <u>every</u> element of $D^{p-1}(\mathbb{K}_p)$ satisfying $(\alpha)(\beta)(\gamma)_{\varepsilon_0}$ can be expressed as $F(t)(dt)^{\otimes(p-1)}$, for <u>some</u> t s.t $\underline{x = \sum_{i\geq 1} a_i t^i}$ $(a_i \in k_p,\ a_1 = 1)$.

(Sketch of proof) First, the differential $\eta^{\otimes(p-1)} \in D^{p-1}(\mathbb{K}_p)$ defined by

$$\eta^{\otimes(p-1)} = \frac{x^2(dx)^{\otimes(p-1)}}{\varepsilon_0 + x^{p+1}}$$

satisfies $(\alpha)(\beta)(\gamma)_{\varepsilon_0}$, because $g(x) = \varepsilon_0$ (constant) satisfies $(\alpha')(\beta')(\gamma')_{\varepsilon_0}$.

Insert $x = \varphi(t) = \sum_{i\geq 1} a_i t^i$ $(a_1 = 1)$ and rewrite $\eta^{\otimes(p-1)}$ in terms of t;

$$\eta^{\otimes(p-1)} = \frac{t^2 (dt)^{\otimes(p-1)}}{g_\varphi(t) + t^{p+1}}.$$

Then
$$g_\varphi(t) = \frac{\varepsilon_0 + \varphi(t)^{p+1}}{(\varphi(t)/t)^2 \varphi'(t)^{p-1}} - t^{p+1}.$$

It suffices to show :

"For any $g(t)$ satisfying $(\alpha')(\beta')(\gamma')_{\varepsilon_0}$ (with t in place of x) there exists $\varphi(t)$ s.t. $g = g_\varphi$".

This follows from termwise approximations based on :

⊚ for any $n \geq 2$. and $\beta \in k_p$,

$$g_{\varphi+\beta t^n} - g_\varphi \equiv (n-2)\,\varepsilon_0 \beta t^{n-1} \pmod{\deg > n-1},$$

which is obtained by straightforward calculations.

(2)

<u>Corollary 1</u> For a given global ω_0, at each $P \in \mathfrak{S}$, we may choose such a local parameter $x_0 = x_{P,0}$ that

$$\omega_0^{\otimes(p-1)} = \frac{x_0^2 (dx_0)^{\otimes(p-1)}}{\varepsilon_0 + x_0^{p+1}}.$$

This is simple and rational in x_0. But not so convenient for finding t_0 s.t. $\omega_0 = d\log t_0$. Looking at the power series for $(1+\varepsilon_0^{-1} x_0^{p+1})^{1/(1-p)} = (1+\varepsilon_0 x^{p+1})^{1+p+p^2+\cdots}$, and throwing away unnecessary terms, keeping the condition $\gamma(\omega_0)=\omega_0$ unaltered, we arrive at the next normalization convenient for finding t_0 s.t. $\omega_0 = d\log t_0$.

(3) As a preparation, consider the p-adic power series [1)]

$$E(z) = \exp\left\{-\left(z+\frac{z^p}{p}+\frac{z^{p^2}}{p^2}+\cdots\right)\right\}$$
$$= \prod_{\substack{n\geq 1\\(n,p)=1}} (1-z^n)^{\mu(n)/n} \qquad (\mu(n): \text{the Möbius } \mu)$$
$$\in \underset{\sim}{\mathbb{Z}}_p[[z]].$$

It satisfies

$$\begin{cases} E'(z)/E(z) = -\theta(z) = -\sum_{n\geq 0} z^{p^n-1}, \\ E(z^p) = \exp(pz)E(z)^p. \end{cases}$$

Let ε be the Teichmüller lift of ε_0 in $\mu_{p-1}\subset \mathbb{Z}_p^\times$. Now, $\theta(z)$ being a power series of z^{p-1} we may put $z^{p-1}=\varepsilon^{-1}x^{p+1}$ and write as

$$\begin{cases} \theta(z) = \vartheta_\varepsilon(x) = \sum_{n\geq 0} \varepsilon^{-n} x^{f_n(p)-1}, \\ f_n(p) = (p+1)\frac{p^n-1}{p-1}+1 \ (= f_n(p) \text{ of } \text{V}-3). \end{cases}$$

(Note that $\varepsilon^{\frac{p^n-1}{p-1}}=\varepsilon^n$.) We have

$$\begin{cases} \vartheta_\varepsilon(x) = 1+\varepsilon^{-1}x^{p+1}\vartheta_\varepsilon(x^p), \\ d\log E(z) = -\theta(z)dz = (\varepsilon^{-1}x^2)^{\frac{1}{p-1}}\vartheta_\varepsilon(x)dx. \end{cases}$$

---

1) cf. [Ddn]; or, [Srr 1] V-17, where $F(z)$ is used for this power series and $E(\ )$ is for the related Artin-Hasse exponential.

(4)

Corollary 2 We can find such a local parameter $x_0^P = x_{P,0}$ for each $P \in \mathfrak{S}$ that

$$\omega_0 = y_0 \vartheta_{\varepsilon_0}(x_0)dx_0 = d\log t_0,$$

for

$$\begin{cases} y_0^{p-1} = \varepsilon_0^{-1} x_0^2, \quad z_0 = x_0 y_0 \\ t_0 = E(z_0). \end{cases}$$

Here, whenever a variable with index n (e.g. $n=0$) is inserted into a power series over $\mathbb{Z}_p$, it means that the value is evaluated mod p^{n+1}.

(5) We shall call $t_0 \in \mathbb{K}_p(\omega_0)^\times$ (or $\mathbb{K}(\omega_0)^\times$) s.t. $\omega_0 = d\log t_0$ "Galois covariant mod$^\times$ A^{p^n}", if for any Galois automorphism δ over $\mathbb{K}_p$ (resp. $\mathbb{K}$),

$$t_0^\delta \cdot t_0^{-\langle\chi_0(\delta)\rangle} \in \mathbb{K}_p(\omega_0)^{p^n} \quad (\text{resp. } \mathbb{K}(\omega_0)^{p^n})$$

holds, where χ: the p-adic character defined by ω_0, $\underset{\sim}{\mu_{p-1}} \ni \chi_0(\delta) \equiv \chi(\delta)$ mod p, and $\underset{\sim}{\mathbb{Z}} \ni \langle\chi_0(\delta)\rangle \equiv \chi_0(\delta)$ mod p^n.

For each given $n \geq 1$, we can always replace t_0 by some "$u^p t_0$" and assume that t_0 is Galois covariant mod$^\times$ A^{p^n}.[1]

In the above case, $t_0 = E(z_0)$ is Galois covariant mod$^\times$ A^{p^n} for each n, because $E(\varepsilon z) = E(z)^\varepsilon$ for any $\varepsilon \in \mu_{p-1}$.

---

1) Because 1-cocycles w.r.t. $Gal(\mathbb{K}(\omega_0)/\mathbb{K}) \curvearrowright \mathbb{K}(\omega_0)^\times / \mathbb{K}(\omega_0)^{\times p}$ split.

(6) Now, suppose *given* a symmetric lifting $\mathfrak{X}_1$ of $\mathfrak{X}_0$. For any closed point P[1] of $\mathbb{X}$, let

$\mathbb{K}_P$: the P-adic completion of $\mathbb{K} = k(\mathbb{X})$,

$\mathfrak{K}_{P,1}$: the R_1-flat local algebra with max. ideal (p), residue field $\mathbb{K}_P$, induced from the local ring $\mathcal{O}_{\mathfrak{X}_1,P}$.

$\sigma_1 = \sigma_{P,1}$: the p-th Frob. on $\mathfrak{K}_{P,1}$ defined by $\mathfrak{X}_1$ at P

ω_0 : the assoc. differential (w.r.t $\pi = p$),

$\mathbb{K}_P^* = \mathbb{K}_P(\omega_0)$,

$\mathfrak{K}_{P,1}^*$: the finite etale ext'n of $\mathfrak{K}_{P,1}$ corresponding to $\mathbb{K}_P^*$;

$t_0 \in (\mathbb{K}_P^*)^\times$ is s.t.

$$\begin{cases} \omega_0 = d\log t_0, \\ t_0 : \text{Galois-covariant mod}^\times \star^{p^2}, \end{cases}$$

$t_1 \in \mathfrak{K}_{P,1}^*$: the unique lifting of t_0 s.t.

$$t_1^{\sigma_1} := t_1^p.$$

$\mathfrak{K}_{P,2}$: the unique R_2-flat local algebra that lifts $\mathfrak{K}_{P,1}$; max. ideal (p)

$\sigma_2 : \mathfrak{K}_{P,2} \to \mathfrak{K}_{P,2}$ any Frobenius which lifts σ_1;

---

1) Here, in (6), P need not belong to $\mathfrak{S}$.

$$\begin{cases} a_0 = a_0(\sigma_2, t_1) \in \mathbb{K}_p^{sep} & (\text{actually} \in \mathbb{K}_p^*); \\ & (\text{cf. Lemma V-1}) \\ \wp(f_0) = a_0, & (f_0 \in \mathbb{K}_p^{sep}), \end{cases}$$

so that $\omega_1 = (d\log t_1)(1 + pf_0)$ is the σ_2-assoc. differential.

By the Galois covar. of t_0, we see that $a_0 \in \mathbb{K}_p$; hence f_0 lies in a p-cyclic extension of $\mathbb{K}_p$.

(7) Now let $P \in \mathfrak{S}$, and let $x_0, y_0, z_0, t_0 = E(z_0)$ be as in Cor. 2; above; thus

$$\omega_0 = d\log t_0, \qquad t_0 = E(z_0) \; \left(\begin{smallmatrix}\text{Gal covar.} \\ \text{mod}^{\times} \star^{p^2}\end{smallmatrix}\right).$$

(In this case $t_1 = E(z_1)$, with a suitable choice of z_1 above z_0, gives the unique ext'n of t_0 s.t. $t_1^{\sigma_1} = t_1^p$; see (8) Step 4, but this is for later purpose.)

Now, the main result of VI-5 is the following

<u>Theorem VI-5</u>. A necessary and sufficient condition for

(*) $\omega_1 = (d\log t_1)(1+p f_0)$ $\quad (\wp(f_0)=a_0\in K_{\mathfrak{P}},\ \gamma(a_0\omega_0)=0)$

to be associated with <u>some</u> <u>local</u> lifting $\mathfrak{X}_2^{\mathfrak{P}}$ of $\mathfrak{X}_1$ $(\mathfrak{P}=(\mathfrak{P}\leftarrow\mathfrak{P}^0\rightarrow\mathfrak{P}'))$

is, for $p\neq 2$, that

(**) $$a_0 \equiv \frac{-2\varepsilon_0}{x_0^{p+1}} + \underset{\mathbb{F}_p}{\overset{\exists}{c_0}} \pmod{x_0\mathcal{O}_{\mathfrak{P}}}.$$

<u>Corollary 1</u> The additive character $\psi_{\mathfrak{P},1}: K_{\mathfrak{P}}^\times \to \mathbb{F}_p$ (VI-4)

is given by

$$\psi_{\mathfrak{P},1}(b) = \mathrm{tr}_{K_{\mathfrak{P}}/\mathbb{F}_p}\ \underset{\mathfrak{P}}{\mathrm{res}}\left(\left(\frac{-2\varepsilon_0}{x_0^{p+1}}+c_0\right)\frac{db}{b}\right) \quad (b\in K_{\mathfrak{P}}^\times).$$

the residue

<u>Corollary 2</u> The p-cyclic subextension of "$K(\omega_1)/K$"

has the conductor exponent $f_1(p) = p+2$.

<u>Remark</u> If one changes x_0 keeping the x_0-expression of ω_0 fixed, then the RHS of (**) may change but this is no contradiction. In fact, both sides depend on t_0. Under $t_0 \to t_0 v_0^p$, they change by $-\wp(d\log v_0/\omega_0)$ (cf. Lemma V-1 (1) for $n=1$).

(8) Outline of the proof of Th VI-5

(Step 1) $\exists x_1$ above x_0 s.t. $x_1^{\sigma_1} = x_1^p - p\varepsilon_0 \vartheta_\varepsilon (x_0^p)^{-1} x_0^{-1}$.

(Step 2) (Normalized Modular Equation) In terms of this x_1 and the corresponding x_1' on $\hat{\mathcal{O}}_{X_1', P'}$, the local equation for X_1^0 above (P, P') has the form

$$(x_1' - x_1^p)(x_1 - x_1'^p) + p\varepsilon_0 (1 - (x_0 x_0')^{p-1}) \varphi_{\varepsilon_0}((x_0 x_0')^p) = 0,$$

where $\varphi_\varepsilon(w) = \vartheta_\varepsilon(w^{\frac{1}{p+1}})^{-1}$

(Step 3) For any x_2, x_2' above x_1, x_1', respectively, let

$$(x_2' - x_2^p)(x_2 - x_2'^p) + p\,\varepsilon_1 (1 - (x_1 x_1')^{p-1}) \varphi_{\varepsilon_1}((x_1 x_1')^p) + p^2 h(x_0, x_0') = 0$$

be the equation for symmetric local extension(s) of $\mathcal{X}_1$ at (P, P'). Here, h runs over those elements of $k_p[[x_0, x_0']]$ that are skew-symmetric w.r.t. the conjugation of $k_p/\mathbb{F}_p$. The corresponding Frobenius σ_2 can be expressed as

$$x_2^{\sigma_2} = x_2^p - p\,\varepsilon_1 \vartheta_{\varepsilon_1}(x_1^p)^{-1} x_1^{-1} + p^2 r_0,$$

with

$$r_0 = (x_0 - x_0^{p^2})^{-1} \cdot \left(\varepsilon_0^2 x_0^{p^2-p-2} \vartheta_{\varepsilon_0}(x_0^p)^{-2} - H(x_0)\right),$$

where $H(x_0) = h(x_0, x_0^p) \in k_p[[x_0]]$. H satisfies $H(0) \in \mathbb{F}_p$, and conversely such an H comes from some h.

(Step 4) Take y_1 above y_0, s.t. $y_1^{\frac{p-1}{2}} = \varepsilon_1^{-1/2} x_1$. — the Teichmüller lift

For $z_1 = x_1 y_1$ and $t_1 = E(z_1)$, we obtain

$$\begin{cases} z_1^{\sigma_1} = z_1^p + p\,\theta(z_0^p)^{-1} z_0, \\ t_1^{\sigma_1} = t_1^p. \end{cases}$$

(Step 5) Take y_2 above y_1, s.t. $y_2^{p-1} = \varepsilon_2^{-1} x_2^2$, $z_2 = x_2 y_2$, and put $t_2 = E(z_2)$. We compute the Frobenius remainders w.r.t. z_2, and then w.r.t. t_2, and obtain the following. Put

$$t_2^{\sigma_2} = t_2^p + p^2 s_0, \qquad \left\{ \begin{array}{l} \xi_0 = -t_0^{-p} ds_0, \\ a_0 = \xi_0/\omega_0 = a_0(\sigma_2, t_1) \end{array} \right\}.$$

Then

$$a_0 = \underset{\substack{|||\\ -\varepsilon^{-1}H(0)}}{\theta_0^{p-1} y_0^p \frac{dr_0}{dz_0}} - \underset{\substack{|||\\ -2}}{2\theta_0^{-1}} \underbrace{- \underset{\substack{|||\\ -2\varepsilon_0 x_0^{-p-1}+2}}{2 z_0^{1-p}\theta_0^{-1-p}}}_{} - \underset{\substack{|||\\ 0}}{z_0 \theta_0^{-1-2p} \theta_0'^{\,p}} \qquad \left(\equiv : \bmod x_0 \mathcal{O}_p\right)$$

where
$$\left(\begin{array}{l} \theta_0 = \theta(z_0) \\ \theta_0' = \dfrac{d\theta_0}{dz_0} \end{array} \right)$$

Hence

$$a_0 \equiv -2\varepsilon_0 x_0^{-p-1} - \varepsilon_0^{-1} H(0) \quad (\bmod x_0 \mathcal{O}_p).$$

Conversely, if $a_0 \equiv -2\varepsilon_0 x_0^{-p-1} + \mathbb{F}_p \pmod{x_0 \mathcal{O}_p}$ and $\gamma(A_0\omega_0) = 0$, then one can reverse the argument and find $H(x_0)$ by "integration", which is possible because $\gamma(A_0\omega_0)=0$. //

VI-6 Local study at $P \notin \mathfrak{S}$

In this case, $\mathrm{ord}_P\, \omega_0^{\otimes(p-1)} = 0$. It is easy to see that one can find in $\mathbb{K}(\omega_0) \otimes_{\mathbb{K}} \mathbb{K}_P$ a generator x_0 of the ideal P s.t. $t_0 = 1 + x_0$ satisfies $\omega_0 = d\log t_0$ and $t_0^{\delta} = t_0^{\chi(\delta)}$ ($\forall \delta \in \mathrm{Gal}(\mathbb{K}(\omega_0)/\mathbb{K})$).

The Frobenius morphism σ_n arising from any local lifting $\mathfrak{X}_n^P$ of $\mathfrak{X}_0$ is "integral", i.e., it maps the completion of the local ring $\mathcal{O}_{X_n,P}$ into itself. (We need not "remove" Π' and hence no denominators appear.) Thus, a_0 w.r.t. t_n (above t_0) is integral and the local character χ_P ($P \notin \mathfrak{S}$) is unramified.

What corresponds to the congruence (**) in Th VI-5, for $P \notin \mathfrak{S}$, is simply

$$(***) \qquad a_0 \equiv 0 \pmod{\mathcal{O}_P}.$$

Incidentally if we drop the assumption $|\mathfrak{S}| = (p-1)(g-1)$ and allow "cusps", then $\mathrm{ord}_P(\omega_0^{\otimes(p-1)}) = -(p-1)$, $t_0 = x_0$, $\omega_0 = d\log x_0$ at each cusp.

VI-7 Global result for the lifting $n=1 \Rightarrow 2$

Theorem VI-7 Let $\mathfrak{X}_1$ be given, with the associated differential ω_0. Choose and fix such $T_0 \in \mathbb{K}(\omega_0)^\times$ that $\omega_0 = d\log T_0$ and that T_0 is Galois covariant mod ${}^\times \bigstar^{p^2}$ (IV-5 (5)). Let $p > 2$.

(I) The following conditions (A) (B) are equivalent.

(A) There exists a symmetric lifting $\mathfrak{X}_2$ of $\mathfrak{X}_1$.

(Recall : $\exists \rightarrow \exists_1$)

(B) There exists $A_0 \in \mathbb{K}$ satisfying (i) (ii);

(i) the formal condition $\gamma(A_0\omega_0) = 0$,

(ii) the local congruences at all $\mathfrak{P}$;

$$(\mathfrak{P} \in \mathfrak{S}) \qquad A_0 \equiv \frac{-2\varepsilon_{\mathfrak{P},0}}{x_{\mathfrak{P},0}^{p+1}} - \wp\left(\frac{d\log v_{\mathfrak{P},0}}{\omega_0}\right) \quad \mathrm{mod}(\mathbb{F}_p + \mathfrak{m}_{\mathfrak{P}}),$$

$$(\mathfrak{P} \notin \mathfrak{S}) \qquad A_0 \equiv -\wp\left(\frac{d\log v_{\mathfrak{P},0}}{\omega_0}\right) \qquad (\mathrm{mod}\ \mathcal{O}_{\mathfrak{P}}),$$

where $x_{\mathfrak{P},0}$, $t_{\mathfrak{P},0}$ are as in VI-5, 6, and $v_{\mathfrak{P},0}^p = T_0 t_{\mathfrak{P},0}^{-1}$.[1)]

(Note : $\exists \rightarrow \exists_1$; because $\gamma(\omega_0) = \omega_0 \neq 0$)

---

1) We note that $\mathrm{ord}_{\mathfrak{P}}\, \wp(*) = p \cdot \mathrm{ord}_{\mathfrak{P}}(*)$, when $\mathrm{ord}_{\mathfrak{P}}(*) \le 0$ $(* = d\log v_{\mathfrak{P},0}/\omega_0)$, that $\mathrm{ord}_{\mathfrak{P}}(*) \ge 0$ for almost all $\mathfrak{P}$, and also that the worst possible value of $\mathrm{ord}_{\mathfrak{P}}(*)$ is -1 except that it can be -2 when $p=3$ <u>and</u> $\mathfrak{P} \in \mathfrak{S}$. (For $p>3$ $\mathfrak{P} \in \mathfrak{S}$, use the Gal. cover. properties w.r.t. a non-triv. inertia elt in $\mathrm{Gal}(\mathbb{K}(\omega_0)/\mathbb{K})$, to conclude that $\mathrm{ord}_{\mathfrak{P}}(d\log v_{\mathfrak{P},0}) = 0$).

(II) When these equivalent conditions are satisfied, the differential associated with $\mathfrak{X}_2$ is given by

$$\omega_1 = (d\log T_1)(1+pF_0) = d\log(T_1 u_0^p),$$

where T_1 is the unique extension[1] of T_0 with $T_1^{\sigma_1} = T_1$, F_0 is a root of the Artin-Schreier equation $\wp(F_0) = A_0$, and $F_0\omega_0 = d\log u_0$.[2]

(Proof) Immediate, by combining

(i) the local-global principle (Th VI-2), (ii) the local result (Th VI-5 ($P\in\mathfrak{S}$), §VI-6 ($P\notin\mathfrak{S}$)), (iii) the formula (Lemma V-1, $n=1$):

$$a_0(\sigma_2, t_1 v_1^p) - a_0(\sigma_2, t_1) = -\wp\left(\frac{d\log v_0}{\omega_0}\right),$$

applied to $T_0 = t_{P,0} v_{P,0}^p$, $A_0 = a_0(\sigma_2, T_1)$. //

<u>Remark 1</u> (i) The RHS of each local congruence (B)(ii) ($P\in\mathfrak{S}$) is independent of the choice of $x_{P,0}$ satisfying Cor 2 VI-5.

(ii) Since this RHS is just a class mod($\mathbb{F}_p + m_P$) etc., in order to compute this for a practical purpose, $x_{P,0}$ need not satisfy the precise equality $\omega_0 = y_0\, \vartheta_{\mathcal{E}_0}(x_0)\, dx_0$ but some congruence, modulo $x_0^n dx_0$ for a suitable power n, suffices.

---

1) To be more precise, if $\mathfrak{k}_1$ is the local ring of X_1 at the generic point and $\sigma_1 : \mathfrak{k}_1 \to \mathfrak{k}_1$: the p-th Frobenius induced from $\mathfrak{X}_1$, T_1 belongs to the subextension of $\tilde{\mathfrak{k}}_1$ corresponding to $\mathbb{K}^* = \mathbb{K}(\omega_0)$.

2) cf. Lemma V-1 (2). Note that "$T_1 u_0^p$" makes sense.

Remark 2 (i) The existence of $A_0 \in \mathbb{K}$ satisfying (B) implies:

$$(*) \qquad \sum_{P\in\mathfrak{S}} \mathrm{tr}_{/\mathbb{F}_p}\, \mathrm{res}_P\left(\frac{-2\varepsilon_{P,0}}{x_{P,0}^{p+1}}\cdot\eta\right) = 0 \qquad \left(\begin{array}{l}\forall\eta\in D(\mathbb{K}), (\eta)\geq 0\\ \underset{\sim\sim\sim}{\gamma(\eta)=\eta}\end{array}\right)$$

(ii)
This necessary condition (*) for $\exists x_2$ is equivalent to the existence of an additive character $\psi_1 : I_K/\mathbb{K}^\times \to \mathbb{F}_p$, unram. outside $\mathfrak{S}$, s.t. for each $P\in\mathfrak{S}$, the restriction $\psi_{P,1} : \mathbb{K}_P^\times \longrightarrow \mathbb{F}_p$ has the form

$$\psi_{P,1}(\ell) = \mathrm{tr}_{K_P/\mathbb{F}_p}\, \mathrm{res}_P\left(\left(\frac{-2\varepsilon_{P,0}}{x_{P,0}^{p+1}} + c_{P,0}\right)\frac{d\ell}{\ell}\right) \qquad (\ell\in\mathbb{K}_P^\times)$$

with some $c_{P,0}\in\mathbb{F}_p$.

(iii)
When ψ_1 exists, the dimension over $\mathbb{F}_p$ of its "freedom" is $1 + \mathrm{rk}\, Cl^{[p]}$, where $Cl^{[p]}$ denotes the p-torsion of the divisor class group of $\mathbb{X}$. ("freedom" involves that of choice of $(c_{P,0})_{P\in\mathfrak{S}}$)

"1" $\longleftrightarrow c\in\mathbb{F}_p$, $(c_{P,0})_P \longrightarrow (c + c_{P,0})_P$)

This analysis taught me that local congruences are not enough. By looking at t_0 instead of just ω_0, I was able to give a result such as Th. VI-7. The formal equality $\gamma(A_0\omega_0) = 0$ was the missing key.

VI-8 Example We take up again Ex. 3 of [20] §3.1.

Let $k = \mathbb{F}_3$, $\mathbb{X}$ the plane quartic $\subset \mathbb{P}^2$ defined by

$$X^3Y - XY^3 + XYZ^2 + aYZ^3 + bXZ^3 + cZ^4 = 0 \quad (a, b, c \in \mathbb{F}_3).$$

(Case 1) $a = b = 0$, $c \neq 0$; (Case 2) $ab \neq 0$; or $a = 0$, $bc \neq 0$. [1)]

In either case, $\mathbb{X}$ is non-singular, with genus $g = 3$. Let

$$\mathfrak{S} = \mathbb{X} \cdot \{Z = 0\} = \{4 \text{ } k\text{-rational pts parametrized by } (X:Y) \in \mathbb{P}^1(k)\}$$

(Note: $(p-1)(g-1) = 4 = |\mathfrak{S}|$)

Let
$$f(x, y) = x^3y - xy^3 + xy + ay + bx + c = 0 \quad (x = X/Z,\ y = Y/Z)$$
be the affine equation. Note that

$$f_x = -(y^3 - y - b), \quad f_y = x^3 + x + a.$$

The differential

$$\omega_0 = f_x^{-1}\, dy = -f_y^{-1}\, dx$$

has the divisor $\mathfrak{S}$, and $\omega_0^{\otimes 2}$ satisfies (A)~(C) of VI-3 (with $\varepsilon_{P,0} = 1$); hence ω_0 is assoc. with a symmetric lifting $\mathcal{X}_1$ of $\mathcal{X}_0 = \{\mathbb{X} \leftarrow \mathbb{X}^0_{\mathfrak{S}} \rightarrow \mathbb{X}\}$.

In [20], it was explained that, in Case 1, $\mathcal{X}_1$ lifts further to a symmetric system $\mathcal{X}$ over $\mathbb{Z}_p$ (as an application of Th 3 (Cor. 1)), and in Case 2 there is no further lifting $\mathcal{X}_2/\mathcal{X}_1$ (by some computation using "ω_1" for this specific case, not mentioned).

---

1) In Case 1, one may (and will) assume $c = 1$.
In Case 2, this strange-looking non-symmetric condition arises because we are considering curves only for $a, b, c \in \mathbb{F}_3$.

Here, we shall give an explicit indication, using Th VI-7, how one can check the liftability of $\mathcal{X}_1$ to $\mathcal{X}_2$ in Case 1, and the non-liftability in Case 2.

(Case 1) Choose $T_0 = \frac{y-y^3}{(x+y)^3}$ as an element satisfying $\omega_0 = d\log T_0$. The divisor $(T_0) = (S_{1,0}/S_{1,-1})^6$, where $S_{\alpha,\beta} \in \mathfrak{S}$ with $(X:Y) = (\alpha:\beta)$. Then $A_0 = T_0 - T_0^{-1}$ satisfies the condition B of Th VI-7; hence $\mathcal{X}_1$ is liftable to $\mathcal{X}_2$ with

$$\omega_1 = (d\log T_1)(1+pF_0), \qquad \delta(F_0) = T_0 - T_0^{-1}$$

(T_1 : the unique ext'n s.t. $T_1^{\sigma_1} = T_1^p$).[1]

(Case 2) In this case, the above choice of T_0 does not make the task simpler. Choose $T_0 = (x^3+x+a)^{-1}$. For each P, let $A_{P,0}$ (here) denote the RHS of the congruence in (B) of Th VI-7. The space of regular differentials on $\mathbb{X}$ is spanned by $\omega_0, x\omega_0, y\omega_0$. If some global $A_0 \in \mathbb{K}$ satisfies the local conditions (B)(ii) for all P, then

$$(*) \qquad \sum_{\text{all } P} \operatorname{tr}_{\mathbb{F}_p}(\operatorname{res}_P(A_{P,0}\,\eta)) = 0$$

must hold for all $\eta \in [\omega_0, x\omega_0, y\omega_0]_{G}$. But this sum $= -b$ for $\eta = y\omega_0$, and $= a$ for $y = x\omega_0$; hence in Case 2 where either $a \neq 0$ or $b \neq 0$, $(*)$ is <u>not</u> satisfied.

1) In this case $\operatorname{ord}_P(d\log v_{P,0}/\omega_0) = -2$ for $P = S_{1,0}, S_{1,-1}$; hence a term of order $-2p = -6$ appears on the RHS of the congruence in Th VI-7.

<u>Remark</u> The divisor of T_0 in Case 2 is $\left(\frac{S_{1,0}S_{1,1}S_{1,-1}}{D}\right)^3$,

$D = R_1R_2R_3$, $R_i \longleftrightarrow \{(x_i, y_i),\ x_i^3 + x_i + a = 0\}$. We have

$A_{P,0} = 0$ for $P \notin \mathfrak{S}^\vee D$, and $\sum_{i=1}^{3} \mathrm{tr}_{/\mathbb{Q}_p} \mathrm{res}_{R_i}(A_{R_i,0}\,\eta) = 0$

for each $\eta = x\omega_0,\ y\omega_0$. For local computations at $P \in \mathfrak{S}^\vee D$,

we need calculations of power series of relevant power series up to

degree 7.

VI-9 Baton pass

As a report of my talks I am afraid I must stop here. If something related can be found I hope to write them down and post new reports in my home page

RIMS home page > staff > emeritus > ...

I thank you for your patience, hope that it was enjoyable at least partly, and strongly hope that the baton can be passed, to YOU.

ihara@kurims.kyoto-u.ac.jp

[References A]

[Crd 1] I.V. Cerednik, Towers of algebraic curves uniformized by discrete subgroups of $PGL_2(k_w) \times E$; Math. USSR Sbornik, 28(1976) No 2, 187-215.

[Crd 2] ————, Uniformization of algebraic curves by discrete arithmetic subgroups of $PGL_2(k_w)$ with compact quotients, ibid, 29(1976) No 1, 55-78.

[Drm] H. Darmon, Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications; Ann. of Math. 154 (2001), 589-639.

[Dlg] P. Deligne, Variétés abéliennes ordinaires sur un corps fini, Invent.math.8 (1969),238-243.

[Drg 1] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper; Abh. Math. Sem.Hamburg Univ. 14(1941), 197-272.

[Drg 2] ————, Invarianten und Normalformen elliptischer Funktionenkörper; Math. Z. 47 (1941), 47-56.

[Ddn] J. Dieudonné, On the Artin-Hasse exponential series,; Proc. AMS 8 (1957), 201-214.

[Ech] M. Eichler, Über die Idealklassenzahl total definiter Quaternionenalgebren; Math. Z. 43 (1938), 102-109.

[Hss 1] H. Hasse, Beweis des Analogons der Riemannschen Vermutung fur die Artinschen und F.K.Schmidtschen Kongruenzzetafunktionen in gewissen Elliptischen Fällen; Nachr.Ger.d.Wiss.Göttingen, Math.Phys. Kl (1933), 253-262

[Hss 2] H.Hasse, Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p; J.r.u.ang.Math. 172(1934),77-85.

[Ig 1] J-I. Igusa, Class number of a definite quaternion with prime discriminant; Proc.Nat.Ac.Sci. U.S.A. 44(1958), 312-314.

[Ig 2] ————,Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves; Amer.J.Math. 81(1959), 453-476.

[Ig 3] ————, On the algebraic theory of elliptic modular functions; J.Math.Soc.Japan 20 (1968), 96-106.

[Ih] Y. Ihara, Non-abelian invariant differentials; Mimeographed Note, 1971 (unpublished)[1] (resume in [Kk] ch 2)

[Kk] M. Koike, Congruences between modular forms and functions and applications to the conjecture of Atkin; J. Fac.Sci. Univ. Tokyo IA 20(1973), 129-169.

[Lbs] J.P.Labesse, Formule des traces et fonction ζ_r de Ihara; Appendice C in "Variété de Shimura et fonctions L", Publ. math. de l'univ. Paris VII (1979),165-178

---

1) available upon request (I try to put a scanned file on my HP at the RIMS(> staff >emeritus > ihara)).

[Lngl] R.P. Langlands, On the zeta-funtions of some simple Shimura varieties, Canadian J. Math. 31-6(1979),1121-1216.

[Mrg 1] G.A.Margulis, Discrete groups of motions of manifolds of nonpositive curvature; (in Russian); Proc.Internat.Congress Math. (Vancouver)2,21-34

[Mrg 2] G.A.Margulis, Discrete subgroups of semisimple Lie groups; Ergebnisse der Mathematik und ihrer Grenzgebiete, Vol 17, Springer, Berlin.

[Mrt] Y. Morita, Reduction mod $\mathfrak{P}$ of Shimura curves, Hokkaido Math. J. 10(1981), 209-238.

[Oht] M. Ohta, On ℓ-adic representations attached to automorphic forms, Jap. J. Math 8 (1982), 1-47.

[Slb] A.Selberg, Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series; J. of the Indian Math.Soc. 20 (1956) 47-87

[Srr1] J-P. Serre, Groupes algébriques et corps de classes, Publ. l'Institute de Mathématique de l'Université de Nancago VII, 1959, Hermann, Paris.

[Srr2] J-P. Serre, Groupes p-divisibles (d'après J. Tate), in "Sem. Bourbaki 19e année 1966/67", No. 318.

[Srr3] J-P. Serre, Arbres, amalgames, SL_2 ; Astérisque 96 soc.math. de france (1977).

[Sh 1] G. Shimura, Construction of class fields and zeta functions of algebraic curves; Ann. of Math. 85(1967), 58-159.

[Sh 2] ———— ,On canonical models of arithmetic quotients of bounded symmetric domains, I. II Ann. of Math.91(1970), 144-222; ibid 92 (1970) 528-549.

[Stk] I. Satake, Spherical functions and Ramanujan Conjecture; AMS Proc. Symp. Pure Math.; Vol. 9(1966), 258-264.

[Tt] J. Tate, Endomorphisms of abelian varieties over finite fields, Invent. math. 2 (1966), 134-144.

[References B]

From the home page of Yasutaka Ihara (伊原康隆)
www.kurims.kyoto-u.ac.jp > Staff > Emeritus >IHARA Yasutaka >Papers List

Papers List (restricted to relevant papers)

1. On certain arithmetical Dirichlet series,
J. Math. Soc. Japan 16 (1964), 214--225.
2. Algebraic curves mod p and arithmetic groups,
Proc. Symp. in pure Math. 9, Amer. Math. Soc. (1966), 265--271.
3. Discrete subgroups of $PL(2,k_p)$
Proc. Symp. in pure Math. 9, Amer. Math. Soc. (1966), 272--278.
4. On discrete subgroups of the two by two projective linear group over p-adic fields,
J. Math. Soc. Japan 18 (1966), 219--235.
5. Hecke polynomials as congruence ζ-functions in elliptic modular case,
Ann. of Math. 85 (1967), 267--297.
6. The congruence monodromy problems,
J. Math. Soc. Japan 20 (1968), 107--121.
7. On congruence monodromy problems, I (1968), II (1969),
Lecture Notes at Univ. of Tokyo; (Russian translation) Matematyka 14-3 (pp.40--98), 14-4 (pp.48--77), 14-5 (pp.62--101) (1970).
8. On congruence monodromy problems, Reproduction of [7], with Author's Notes (2008); MSJ Memoirs 18, Math. Soc. Japan (2008).
9. An invariant multiple differential attached to the field of elliptic modular functions of characteristic p,
Amer. J. Math. XCIII (1971), 139--147.
10. Non-abelian classfields over function fields in special cases,
Actes du congres international des mathematiciens, Tome 1, Nice, (1970), 381-389.
11. On ($\infty \times p$)-adic coverings of curves,
Proc. Internat. Conf. on Number theory, Moscow, Sept. 1971; Trudy Math. Inst. Steklov 132 (1973), 118--131.
12. On modular curves over finite fields,
Papers presented at the Internat. Colloquim on Discrete Subgroups and applications to the problem of Moduli;
Bombay, Jan. 1973; Tata Inst. Fund. Studies, Oxford Univ. Press; 161--202.
13. Schwarzian equations,
J. Fac. Sci. Univ. of Tokyo IA 21 (1974), 97--118.
14. On the differentials associated to congruence relations and the Schwarzian equations defining uniformizations,
J. Fac. Sci. Univ. of Tokyo IA 21 (1974), 309--332.
15. (with Hiroo Miki) Criteria related to potential unramifiedness and reduction of unramified coverings of curves,
J. Fac. Sic. Univ. of Tokyo IA 22 (1974), 237--254.

16. Some fundamental groups in the arithmetic of algebraic curves over finite fields,
Proc. Nat. Acad. Sci. U.S.A. 72 (1975), 3281--3284.

17. On the Frobenius correspondences of algebraic curves,
Proc. Internat. Symp. on Alg. Number Theory, Kyoto (1976); 67--98, Japan Soc. of Promotion of Science.

18. Congruence relations and Shimura curves I,
Proc. Symp. in pure Math. 33 (Part 2), Amer. Math. Soc. (1979), 291--311.

19. Congruence relations and Shimura curves II,
J. Fac. Sci. Univ. Tokyo IA 25 (1979), 301--361.

20. Lifting curves over finite fields together with the characteristic correspondence Π + Π',
J. Algebra 75 (1982), 452--483.

21. Congruence relations and fundamental groups,
J. Algebra 75 (1982), 445--451.

22. Some remarks on the number of rational points of algebraic curves over finite fields,
J. Fac. Sci. Univ. of Tokyo, IA 28 (1982), 721--724.

23. On unramified extensions of function fields over finite fields,
Adv. Studies in Pure Math. Vol.2 (1983), 89--97, Kinokuniya, North Holland.

24. How many primes decompose completely in an infinite unramified Galois extensions of a global field?
J. Math. Soc. Japan 35 (1983), 694--709.

---

25. Profinite braid groups, Galois representations and complex multiplications,
Ann. of Math. 123 (1986), 43--106.

26 On Galois representations arising from towers of coverings of $\mathbb{P}^1 - \{0,1,\infty\}$
Invent. Math. 86 (1986), 427--459.

---

47. Shimura curves over finite fields and their rational points;
in ``Applications of Curves over Finite Field" (ed. M. Fried), Contemporary Math. 245 (1999), 15-23.

62. Comparison of some quotients of fundamental groups of algebraic curves over *p*-adic fields, Adv. Studies in Pure Math. 63 (2012), 221-249;

Galois-Teichmüller Theory and Arithmetic Geometry.

Research Institute for Mathematical Sciences , Kyoto University,
Kyoto, 606-8502 JAPAN FAX: +81-75-753-7272