Universal deformations, rigidity, and Ihara's cocycle

Colin Stewart

Department of Mathematics and Statistics

McGill University, Montréal

January, 2001

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfilment of the requirements of the degree of Master of Science.

Abstract

In [Iha86b], Ihara constructs a universal cocycle

$$\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathbb{Z}_p[[t_0, t_1, t_\infty]]/\left((t_0+1)(t_1+1)(t_\infty+1)-1\right)$$

arising from the action of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ on certain quotients of the Jacobians of the Fermat curves

$$x^{p^n} + y^{p^n} = 1$$

for each $n \geq 1$. This thesis gives a different construction of part of Ihara's cocycle by considering the universal deformation of certain two-dimensional representations of $\Pi_{\overline{\mathbb{Q}}}$, where $\Pi_{\overline{\mathbb{Q}}}$ is the algebraic fundamental group of $\mathbb{P}^1(\overline{\mathbb{Q}}) \setminus \{0, 1, \infty\}$. More precisely, we determine, with and without certain deformation conditions, the universal deformation ring arising from a residual representation

$$\bar{\rho} : \Pi_{\overline{\mathbb{Q}}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_p).$$

Belyĭ's Rigidity Theorem is used to extend each determinant one universal deformation to a representation of Π_K, where K is a finite cyclotomic extension of $\mathbb{Q}(\mu_{p^\infty})$. For a particular $\bar{\rho}$, we give a geometric construction of one such extended universal deformation ρ, and show that part of Ihara's cocycle can be recovered by specializing ρ at infinity.

Résumé

Dans [Iha86b], Ihara construit un cocycle universel

$$\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathbb{Z}_p[[t_0, t_1, t_\infty]]/\left((t_0+1)(t_1+1)(t_\infty+1)-1\right)$$

provenant de l'action de $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ sur certains quotients des jacobiennes des courbes de Fermat

$$x^{p^n} + y^{p^n} = 1$$

pour chaque $n \geq 1$. Cette thèse présente une construction différente d'un cas particulier du cocycle d'Ihara en considérant la déformation universelle de certaines représentations de dimension deux de $\Pi_{\overline{\mathbb{Q}}}$, où $\Pi_{\overline{\mathbb{Q}}}$ est le groupe fondamental de $\mathbb{P}^1(\overline{\mathbb{Q}}) \setminus \{0, 1, \infty\}$. Plus précisement, nous décrivons, avec et sans certaines conditions de déformation, l'anneau de déformation universelle provenant d'une représentation residuelle

$$\bar{\rho} : \Pi_{\overline{\mathbb{Q}}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_p).$$

Le théorème de rigidité de Belyĭ est utilisé pour étendre chaque déformation universelle de déterminant un à une représentation du groupe Π_K, où K est une extension cyclotomique de degré fini de $\mathbb{Q}(\mu_{p^\infty})$. Pour un $\bar{\rho}$ particulier, une construction géométrique d'une de ces déformations universelles étendues ρ est fournie. Ceci permet de récupérer un cas particulier du cocycle d'Ihara par spécialisation de ρ à l'infini.

Acknowledgments

First and foremost, I would like to thank my supervisor, Henri Darmon, for his boundless patience and optimism, and for always finding the time to give me help when I needed it. I am also grateful to him for suggesting this project, which has allowed me to encounter a wide range of beautiful mathematics. My brother, Ian Stewart, has also earned my gratitude for his many helpful editorial suggestions, and for lending his expertise with LaTeX. In addition, I would like to thank Eyal Goren for a number of stimulating discussions, Marc-Hubert Nicole for his help with translating the abstract, and, not least of all, Laura Mark for her encouragement and distractions. Finally, I would like to thank NSERC for their generous financial support of this research.

Contents

1 Introduction

One approach to studying the absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ has been via its canonical representation in the outer automorphism group of the algebraic fundamental group $\Pi_{\overline{\mathbb{Q}}}$ of $\mathbb{P}^1(\overline{\mathbb{Q}}) \setminus \{0, 1, \infty\}$. Let M denote the maximal algebraic extension of $\overline{\mathbb{Q}}(t)$ unramified outside $t = 0, 1, \infty$. Conjugating in $\mathrm{Gal}\,(M/\mathbb{Q}(t))$ by a lift of $\gamma \in G_{\mathbb{Q}}$ gives rise to an automorphism of $\Pi_{\overline{\mathbb{Q}}}$ whose class modulo the group of inner automorphisms depends only on γ. Thus $G_{\mathbb{Q}}$ acts on $\Pi_{\overline{\mathbb{Q}}} = \mathrm{Gal}\left(M/\overline{\mathbb{Q}}(t)\right)$ as a group of outer automorphisms, and we obtain a representation

$$\phi : G_{\mathbb{Q}} \longrightarrow \mathrm{Out}\left(\Pi_{\overline{\mathbb{Q}}}\right).$$

By a theorem of Belyĭ, ϕ is injective; as a result, studying the full representation ϕ seems to be too difficult. However, as a first step in this direction, Ihara considered, for each prime p, the representation

$$\psi : G_{\mathbb{Q}} \longrightarrow \mathrm{Out}\,(\mathcal{F}/\mathcal{F}''),$$

where $\mathcal{F}$ denotes the maximal pro-p quotient of $\Pi_{\overline{\mathbb{Q}}}$, and $\mathcal{F}'' = [[\mathcal{F}, \mathcal{F}], [\mathcal{F}, \mathcal{F}]]$ denotes the double commutator subgroup of $\mathcal{F}$. We define a $\mathbb{Z}_p$-algebra $\mathcal{A}$ by

$$\mathcal{A} = \mathbb{Z}_p[[t_0, t_1, t_\infty]]/\left((t_0 + 1)(t_1 + 1)(t_\infty + 1) - 1\right).$$

Letting $\chi_p : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_p^{\times}$ denote the p-cyclotomic character, $G_{\mathbb{Q}}$ acts as $\mathbb{Z}_p$-algebra automorphisms on $\mathcal{A}$ by

$$\gamma \cdot (1+t_i) = (1+t_i)^{\chi_p(\gamma)}$$

for each $\gamma \in G_{\mathbb{Q}}$, and each $i = 0, 1, \infty$. In [Iha86b], Ihara shows that ψ is encoded by a cocycle

$$F : G_{\mathbb{Q}} \longrightarrow \mathcal{A}^{\times}.$$

For each n, F describes in a precise way the action of $G_{\mathbb{Q}(\mu_{p^n})}$ on the p-adic Tate module of the primitive quotients of the Jacobian of the Fermat curve $F_n : x^{p^n} + y^{p^n} = 1$ (see Theorem 5.4).

Let $r : \mathcal{A} \longrightarrow \mathbb{Z}_p[[T]]$ be the $\mathbb{Z}_p$-algebra homomorphism which maps t_0 and t_1 to T. In this paper, we describe a new construction of $r \circ F$ for each odd p, obtained via deformation theory of two-dimensional representations of $\Pi_{\overline{\mathbb{Q}}}$ and the rigidity method of Belyĭ, Matzat, and Thompson.

We begin in Chapter 2 by considering deformations of arbitrary absolutely irreducible residual representations

$$\bar{\rho} : \Pi_{\overline{\mathbb{Q}}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_p).$$

First we consider general deformations, then deformations subject to certain conditions; namely, the condition of having determinant equal to one, as well as certain "ordinariness" conditions combined with this determinant condition (see §2.6 for precise definitions). In each case, we determine the universal deformation ring, which is a power series ring with coefficients in $\mathbb{Z}_p$, where the number of parameters depends only on the deformation conditions (see Theorems 2.27 to 2.31). In particular, let $\sigma_0, \sigma_1, \sigma_\infty \in \Pi_{\overline{\mathbb{Q}}}$ be topological generators of inertia groups above $t = 0, 1, \infty$ respectively, satisfying $\sigma_0\sigma_1\sigma_\infty = 1$; then if $\bar{\rho}$ has determinant one and is $\{\sigma_0, \sigma_1\}$-ordinary, the $\{\sigma_0, \sigma_1\}$-ordinary determinant one universal deformation ring of $\bar{\rho}$ is the power series ring $\mathbb{Z}_p[[T]]$.

The arithmetic content of the various determinant one universal deformations $(R^{\mathrm{univ}}, \rho^{\mathrm{univ}})$ of Chapter 2 arises in Chapter 3 by means of rigidity. In order to use Belyĭ's Rigidity Theorem (Theorem 3.5) to extend these universal deformations, we study rigidity in $\mathrm{GL}_2(R)$, where R is a local unique factorization domain, proving in particular that $\left(\rho^{\mathrm{univ}}(\sigma_0), \rho^{\mathrm{univ}}(\sigma_1), \rho^{\mathrm{univ}}(\sigma_\infty)\right)$ is rigid in $\mathrm{GL}_2(R^{\mathrm{univ}})$ (see Theorem 3.10). This result allows us to extend each representative of ρ^{univ} to a representation of $\Pi_{K(t)} := \mathrm{Gal}\,(M/K(t))$, where K is a cyclotomic extension of $\mathbb{Q}(\mu_{p^\infty})$ of degree at most $p^2 - 1$ which depends on $\bar{\rho}$ (see Theorem 3.12).

In Chapter 4, we fix the residual representation $\bar{\rho}$ to be the representation describing the action of $\Pi_{\overline{\mathbb{Q}}}$ on the p-torsion points of the Legendre family E_L of elliptic curves given by

$$E_L : y^2 = x(x-1)(x-t).$$

In this case, $\bar{\rho}$ is $\{\sigma_0, \sigma_1\}$-ordinary, and the extension theorem of Chapter 3 shows that any representative of the $\{\sigma_0, \sigma_1\}$-ordinary universal deformation of $\bar{\rho}$ can be extended to a representation

$$\rho : \Pi_{\mathbb{Q}(\mu_{p^\infty})} \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}_p[[T]]\right).$$

Let μ_{p^n} be the group of p^nth roots of unity in $\overline{\mathbb{Q}}$, and let $\mathbb{Z}_p[\mu_{p^n}]$ be the corresponding group ring. We construct ρ as the inverse limit of the representations

$$\rho_n : \Pi_{\mathbb{Q}(\mu_{p^\infty})} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_p[\mu_{p^n}])$$

associated to the curves $C_n/\mathbb{Q}(t)$ given by

$$C_n : y^2 = x\left(x^{2p^n} + (4t-2)x^{p^n} + 1\right),$$

where the action of μ_{p^n} on C_n is given by $\zeta_n \cdot (x, y) = (\zeta_n x, \zeta_n^{\frac{p^n+1}{2}} y)$ for any primitive p^nth root of unity ζ_n. In order to obtain a detailed understanding of each ρ_n, we make use of Mumford's uniformization (Theorem 4.11) of Jacobians of curves C/L having a specific reduction type, where L is a field which is complete with respect to a non-archimedean valuation. We also use a general theorem of Katz (Theorem 4.31) which gives a geometric construction of any representation

$$\kappa : \Pi_{\overline{\mathbb{Q}}} \longrightarrow \mathrm{GL}_2\left(\mathbb{Q}_p(\zeta_n)\right)$$

for which $(\kappa(\sigma_0), \kappa(\sigma_1), \kappa(\sigma_\infty))$ is rigid.

Finally, we show in Chapter 5 how to specialize ρ at ∞ so as to obtain the representation $r \circ F$ (see Theorem 5.7). To prove that these representations are equal, we use the geometric construction of Chapter 4 to show that the given specialization ρ_∞ of ρ describes the action of $G_{\mathbb{Q}(\mu_{p^\infty})}$ on certain quotients of the Jacobian J_n of the Fermat curve F_n. This property together with the corresponding property of $r \circ F$ implies that $r \circ F$ is a direct summand of ρ_∞.

This thesis is comprised of a combination of known and original results. Whenever possible, I have listed a source for known results. The main results of Chapter 2, namely Theorem 2.27 and the results contained in §2.6, may be known to some people, but, to my knowledge, have not previously been written down. The theorems of §§3.3 and 3.4 are original, as are all results appearing after Proposition 4.25 except those that are clearly marked otherwise.

2 Deformation Theory of $\Pi_{\overline{\mathbb{Q}}}$

2.1 Profinite Groups and Infinite Galois Theory

Throughout the sequel, we will be working extensively with Galois groups of infinite Galois extensions. In this section, we present the basic theory of such extensions, and show how profinite groups arise naturally as Galois groups in this context.

Let $(I, \leq)$ be a *directed set*, that is, $\leq$ is a partial order on I such that for each $i, j \in I$, there is some $k \in I$ such that $i \leq k$ and $j \leq k$.

Definition 2.1 *A* directed system *of groups* $(G_i, (\phi_{ji}))$ *is a collection of groups* $\{G_i\}_{i \in I}$ *indexed by* I*, together with homomorphisms* $\phi_{ji} : G_j \longrightarrow G_i$ *for each* $i \leq j$ *such that* $\phi_{ii} = \mathrm{Id}_{G_i}$ *and* $\phi_{ki} = \phi_{ji} \circ \phi_{kj}$ *for* $i \leq j \leq k$*.*

Given a directed system of groups $(G_i, (\phi_{ji}))$, a group G together with homomorphisms $g_i : G \longrightarrow G_i$ for each $i \in I$ will be called a *commuting system above* $(G_i, (\phi_{ji}))$ if the diagrams

$$\begin{tikzcd} & G \arrow[dl, "g_j"'] \arrow[dr, "g_i"] & \\ G_j \arrow[rr, "\phi_{ji}"'] & & G_i \end{tikzcd}$$

commute for all $i \leq j$.

Proposition 2.2 *Given a directed system of groups* $(G_i, (\phi_{ji}))$*, there is a commuting system* $(G, (g_i))$ *above* $(G_i, (\phi_{ji}))$ *satisfying the following universal property: given any commuting system* $(H, (f_i))$ *above* $(G_i, (\phi_{ji}))$*, there exists* *a unique homomorphism $f : H \longrightarrow G$ such that the diagram*

$$\begin{tikzcd} & H \arrow[d, "f"] \arrow[ddl, bend right, "f_j"'] \arrow[ddr, bend left, "f_i"] & \\ & G \arrow[dl, "g_j"'] \arrow[dr, "g_i"] & \\ G_j \arrow[rr, "\phi_{ji}"'] & & G_i \end{tikzcd}$$

commutes for all $i \leq j$.

Proof: Take G to be the set of all sequences of elements of $\{G_i\}_{i \in I}$ compatible under the maps ϕ_{ji}; that is

$$G = \left\{ (\sigma_i)_{i \in I} \in \prod_{i \in I} G_i : \sigma_i \in G_i, \phi_{ji}(\sigma_j) = \sigma_i \text{ for all } i \leq j \right\}.$$

Then G is a subgroup of $\prod\limits_{i \in I} G_i$ and satisfies the given universal property (see [Mor96], App. C, Proposition 4.2 for details). $\square$

Remark: By the usual argument for universal objects, $(G, (g_i))$ is unique up to unique isomorphism (see, e.g., [Lan93], p.57). We write $G = \varprojlim\limits_{i \in I} G_i$, and call $(G, (g_i))$ the *inverse limit* of $(G_i, (\phi_{ji}))$.

By the same construction, inverse limits exist in the categories of rings, modules, and topological groups, among others.

Definition 2.3 *A* profinite group *is a group which can be expressed as the inverse limit of a directed system of finite groups. A profinite group is said to be* procyclic *if it can be expressed as the inverse limit of a directed system of finite cyclic groups.*

Given a profinite group $G = \varprojlim G_i$ (where each G_i is finite), we may view

G as a subgroup of the direct product $\prod_{i \in I} G_i$ as in the proof of Proposition 2.2 above. Giving each G_i the discrete topology, we may define a topology on G by taking the topology induced from the product topology on $\prod_{i \in I} G_i$. This definition gives G the structure of a topological group, and plays an essential role in the theory of infinite Galois extensions. For more on profinite groups, see [Sha72].

Consider an infinite Galois extension L/K. Let $G = \mathrm{Gal}\,(L/K)$. Given any finite Galois extension M/K contained in L, the group $G_M := \mathrm{Gal}\,(L/M)$ is a normal subgroup of G of finite index $[M : K]$, and G/G_M is isomorphic to $\mathrm{Gal}\,(M/K)$, as in the case of finite extensions. Let $\mathcal{M}$ denote the set of all such intermediate fields M. Then $\mathcal{M}$ forms a directed set by inclusion, and $\{G/G_M\}_{M \in \mathcal{M}}$ together with the canonical maps $\phi_{M'M} : G/G_{M'} \longrightarrow G/G_M$ whenever $G_{M'} \subset G_M$ (i.e. whenever $M' \supset M$) forms a directed system of finite groups. The canonical maps $G \longrightarrow G/G_M$ define a commuting system above $(G/G_M, (\phi_{M'M}))$, so by the universal property of the inverse limit, we obtain a homomorphism $\phi : G \longrightarrow \varprojlim_{M \in \mathcal{M}} G/G_M$. In fact, ϕ is an isomorphism (see [Lan93], Ch. VI, Theorem 14.1). Thus G is naturally a profinite group. The topology on G is called the *Krull topology*. The Krull topology may also be defined without realizing G as a profinite group by taking as a base for open sets $\{\sigma G_M : \sigma \in G, M \in \mathcal{M}\}$.

As with finite Galois extensions, one defines the *Galois correspondence* between the set of intermediate fields M between K and L, and the set of subgroups H of $G = \mathrm{Gal}\,(L/K)$. This correspondence takes the intermediate field M to the subgroup $\mathrm{Gal}\,(L/M)$, and the subgroup H to the intermediate field L^H consisting of those elements of L fixed pointwise by H. In the case of infinite Galois extensions, not every subgroup of G arises as $\mathrm{Gal}\,(L/M)$ for some intermediate field M. However, the Krull topology on G allows us to identify which subgroups correspond to intermediate fields, in a way which is made precise by the Fundamental Theorem of Infinite Galois Theory:

Theorem 2.4 *The Galois correspondence defines an inclusion-reversing bijection between the set of closed subgroups of G and the set of intermediate fields between K and L. Moreover, a closed subgroup $H \subset G$ is normal if and only if the corresponding extension L^H/K is Galois, in which case* $\mathrm{Gal}\left(L^H/K\right) \cong G/H$*, the isomorphism being one of topological groups if we give G/H the quotient topology.*

Outline of Proof: The main observation is that given any subgroup $H \subset G$, $\mathrm{Gal}\left(L/L^H\right) = \overline{H}$, where $\overline{H}$ denotes the closure of H in G with respect to the Krull topology. This observation together with the usual fundamental theorem of Galois theory reduces the proof to verifying certain details, which may be found in [Mor96], Ch. IV, §17. $\square$

Given any group G, let $\mathcal{N}$ denote the set of all normal subgroups of G of finite index. Then $\mathcal{N}$ is naturally a directed set with respect to inclusion, and $\{G/N\}_{N \in \mathcal{N}}$ together with the canonical homomorphisms forms a directed system of finite groups.

Definition 2.5 *For any group G, the profinite group*

$$\widehat{G} := \varprojlim_{N \in \mathcal{N}} G/N$$

is called the profinite completion *of G.*

The profinite completion of a group is indeed a topological completion in the usual sense; it is possible to define Cauchy sequences in G with respect to a directed set of normal subgroups, in which case $\widehat{G}$ is the completion of G with respect to these sequences. See [Lan93], Ch. I, §10 for details.

It is often useful to consider the subset $\mathcal{N}_p$ of $\mathcal{N}$ consisting of all normal subgroups of G of p-power index, where p is a fixed prime. In this case, $\varprojlim_{N \in \mathcal{N}_p} G/N$ is called the *pro-p completion* of G. A collection of elements $\{\gamma_i\}_{i \in I}$ of a profinite group G is said to *topologically generate* G if the subgroup of G generated by $\{\gamma_i\}_{i \in I}$ is dense in G. Thus, for example, if $\widehat{G}$ is the profinite completion of a group G, and $\{\gamma_i\}_{i \in I}$ generates G, then viewing each γ_i as an element of $\widehat{G}$ via the natural map $G \longrightarrow \widehat{G}$, the system $\{\gamma_i\}_{i \in I}$ topologically generates $\widehat{G}$.

2.2 The Algebraic Fundamental Group

In this section, we give an explicit description of the group structure of $\mathrm{Gal}\big(K/\overline{\mathbb{Q}}(t)\big)$, where K is the maximal algebraic extension of the function field $\overline{\mathbb{Q}}(t)$ ramified only at a fixed finite set of places.

Given fields K and F, and a place $\phi : K \longrightarrow F \cup \{\infty\}$, the set $\phi^{-1}(F)$ of finite elements under ϕ is a local subring R of K with maximal ideal $\mathfrak{p} = \phi^{-1}(0)$. We call R the *valuation ring* corresponding to ϕ, and $\mathfrak{p}$ its *valuation ideal.* If V/K is a variety with function field $K(V)$, one may define a place $\phi_P : K(V) \longrightarrow K \cup \{\infty\}$ for each point $P \in V$ by $\phi_P(f) = f(P)$, where we let $f(P) = \infty$ if f is not defined at P. In this case, the valuation ideal of ϕ_P is also called the valuation ideal corresponding to P.

Let L/K be a (possibly infinite) Galois extension. Let $\mathfrak{p}$ be a valuation ideal of K, and suppose that $\widehat{\mathfrak{p}}$ is a valuation ideal of L lying above $\mathfrak{p}$, with corresponding valuation ring $A \subset L$.

Definition 2.6 *The group*

$$D\left(\widehat{\mathfrak{p}}/\mathfrak{p}\right) := \{\sigma \in \mathrm{Gal}\,(L/K) : \sigma(\widehat{\mathfrak{p}}) = \widehat{\mathfrak{p}}\}$$

is called the decomposition group *of* $\widehat{\mathfrak{p}}/\mathfrak{p}$. *The* inertia group $I\left(\widehat{\mathfrak{p}}/\mathfrak{p}\right)$ *of* $\widehat{\mathfrak{p}}/\mathfrak{p}$ *is the subgroup of* $D\left(\widehat{\mathfrak{p}}/\mathfrak{p}\right)$ *given by*

$$I\left(\widehat{\mathfrak{p}}/\mathfrak{p}\right) := \{\sigma \in \mathrm{Gal}\,(L/K) : \sigma(a) \equiv a \mod \widehat{\mathfrak{p}} \text{ for all } a \in A\}.$$

We say that $\widehat{\mathfrak{p}}$ *is* unramified *over* $\mathfrak{p}$ *if* $I\left(\widehat{\mathfrak{p}}/\mathfrak{p}\right) = 1$.

If every valuation ideal of L lying above $\mathfrak{p}$ is unramified over $\mathfrak{p}$, then we say that $\mathfrak{p}$ is unramified in L. We will also say that a place ϕ of K is unramified in L if the valuation ideal corresponding to ϕ is unramified in L.

Let k be an algebraically closed subfield of $\mathbb{C}$. Let $P_1, \dots, P_r$ be distinct points in $\mathbb{P}^1(k)$, and $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ their corresponding valuation ideals in $k(t)$. Let $k(t)_S$ denote the maximal algebraic extension of $k(t)$ unramified outside $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$. Give $\mathbb{P}^1(\mathbb{C})$ the topology of the Riemann sphere, and choose a point $P \in \mathbb{P}^1(\mathbb{C}) \setminus \{P_1, \dots, P_r\}$. Let Π be the topological fundamental group $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{P_1, \dots, P_r\}, P) \cong \langle \gamma_1, \dots, \gamma_r \mid \gamma_1 \cdots \gamma_r = 1 \rangle$.

Theorem 2.7 *The extension* $k(t)_S/k(t)$ *is Galois and* $\mathrm{Gal}\,(k(t)_S/k(t))$ *is isomorphic to the profinite completion* $\widehat{\Pi}$ *of* Π. *Moreover, there are generators* $\gamma_1, \dots, \gamma_r$ *of* Π *such that for each* $i = 1, \dots, r$, *the image of* γ_i *in*

$\mathrm{Gal}\,(k(t)_S/k(t))$ *topologically generates the (procyclic) inertia group* $I\left(\widehat{\mathfrak{p}}_i/\mathfrak{p}_i\right)$ *of some valuation ideal* $\widehat{\mathfrak{p}}_i$ *above* $\mathfrak{p}_i$.

Outline of Proof: First assume $k = \mathbb{C}$. Then there exists a universal covering $u : U \longrightarrow \mathbb{P}^1(\mathbb{C}) \setminus \{P_1, \ldots, P_r\}$. Using the Riemann Existence Theorem, one may show that finite Galois extensions $N/k(t)$ unramified outside S are in bijective correspondence with finite coverings $p : Y \longrightarrow \mathbb{P}^1(\mathbb{C})$ of compact Riemann surfaces unramified outside $\{P_1, \ldots, P_r\}$ in such a way that the surface Y corresponds to its function field $N/k(t)$ (see [Vol96], Theorem 5.14). Moreover, $\mathrm{Gal}\,(N/k(t))$ is isomorphic to the group $\mathrm{Deck}(p)$ of deck transformations of the covering p. Now $\tilde{p} := p|_{Y \setminus p^{-1}(\{P_1,\ldots,P_r\})}$ is a covering of $\mathbb{P}^1(\mathbb{C}) \setminus \{P_1, \ldots, P_r\}$, and $\mathrm{Deck}(p) \cong \mathrm{Deck}(\tilde{p})$. Using the universal covering u above, one sees that such coverings $\tilde{p}$ are in bijective correspondence with normal subgroups H of Π of finite index in such a way that $\mathrm{Deck}(\tilde{p}) \cong \Pi/H$. Thus, letting $\mathcal{N}_{k,S} = \{N \subset k(t)_S : N/k(t) \text{ is finite, Galois}\}$, we have

$$\begin{aligned} \mathrm{Gal}\,(k(t)_S/k(t)) &\cong \varprojlim_{N \in \mathcal{N}_{k,S}} \mathrm{Gal}\,(N/k(t)) \\ &\cong \varprojlim_{\substack{H \lhd \Pi \\ \text{finite index}}} \Pi/H = \widehat{\Pi}. \end{aligned}$$

This proves the first statement when $k = \mathbb{C}$.

To prove the second statement when $k = \mathbb{C}$, let Y and N be as above, fix a point $\widehat{P} \in u^{-1}(P)$, and let $\tilde{P} \in Y$ be the image of $\widehat{P}$. It is possible to choose lifts $\tilde{P}_i \in Y$ of each P_i, and $d_i \in \mathrm{Deck}(p)$ so that $d_i(\tilde{P}_i) = \tilde{P}_i$ and $d_1 \circ \cdots \circ d_r = \mathrm{Id}$. Let $\bar{\mathfrak{p}}_i$ be the valuation ideal in N corresponding to $\tilde{P}_i$. Let $\sigma_i \in \mathrm{Gal}\,(N/k(t))$ be the automorphism satisfying $\sigma_i\left(f(\tilde{P})\right) = d_i(\tilde{P})$ for

$f \in N$. Then σ_i generates $I(\bar{\mathfrak{p}}_i/\mathfrak{p}_i)$, and the various σ_i obtained in this way are compatible as N varies over finite extensions of $k(t)$. Viewing $\mathrm{Gal}(k(t)_S/k(t))$ as the inverse limit $\varprojlim_{N \in \mathcal{N}_{k,S}} \mathrm{Gal}(N/k(t))$ and taking $\gamma_i = (\sigma_i)_{N \in \mathcal{N}_{k,S}}$ gives generators of $\mathrm{Gal}(k(t)_S/k(t))$ satisfying the assertions of the theorem with $\widehat{\mathfrak{p}}_i = \bigcup_{N \in \mathcal{N}_{k,S}} \bar{\mathfrak{p}}_i$. This proves the theorem when $k = \mathbb{C}$.

For any algebraically closed subfield k of $\mathbb{C}$, let S' denote the set of valuation ideals in $\mathbb{C}(t)$ corresponding to the points $P_1, \ldots, P_r \in \mathbb{P}^1(k) \subset \mathbb{P}^1(\mathbb{C})$. One may show that the assignment $N \longmapsto N \otimes_k \mathbb{C}$ defines a bijection $\mathcal{N}_{k,S} \longrightarrow \mathcal{N}_{\mathbb{C},S'}$. This bijection gives rise to an isomorphism

$$\begin{aligned}
\mathrm{Gal}(k(t)_S/k(t)) &\cong \varprojlim_{N \in \mathcal{N}_{k,S}} \mathrm{Gal}(N/k(t)) \\
&\cong \varprojlim_{N \otimes_k \mathbb{C} \in \mathcal{N}_{\mathbb{C},S'}} \mathrm{Gal}(N \otimes_k \mathbb{C}/\mathbb{C}(t)) \\
&\cong \mathrm{Gal}(\mathbb{C}(t)_S/\mathbb{C}(t)),
\end{aligned}$$

as desired. See [MM99], Ch. I, Theorems 1.3, 1.4, and 2.2 for full details. □

Remark: The above theorem is true for any algebraically closed field k of characteristic 0. We will only need the result when $k = \overline{\mathbb{Q}}$.

Theorem 2.7 is part of a much more general connection between Galois groups over function fields and topological fundamental groups. Let k be as above, and X/k a smooth projective curve of genus g. Given distinct points $P_1, \ldots, P_r \in X(k)$, the maximal algebraic extension $k(X)_S$ of the function field $k(X)$ of X unramified outside the set S of valuation ideals of $P_1, \ldots, P_r$ is Galois. The group $\mathrm{Gal}(k(X)_S/k(X))$ is called the *algebraic fundamental group* of $X \setminus \{P_1, \ldots, P_r\}$, and is denoted by $\pi_1^{\mathrm{alg}}(X \setminus \{P_1, \ldots, P_r\})$. There is, up to homeomorphism, a unique compact connected oriented surface X_g of genus g (see, e.g. [Arm97], §7.4, 7.5). Theorem 2.7 may be generalized to this context as follows: let $Q_1, \ldots, Q_r \in X_g$ be distinct points, and choose any point $Q \in X_g \setminus \{Q_1, \ldots, Q_r\}$; then $\pi_1^{\mathrm{alg}}(X \setminus \{P_1, \ldots, P_r\})$ is isomorphic to the profinite completion of $\pi_1(X_g \setminus \{Q_1, \ldots, Q_r\}, Q)$. See [Ser92], §6.3 for more details.

2.3 The $\mathfrak{m}$-adic Topology

This section collects some results concerning rings with which we will be working below. All rings will be assumed to be commutative.

Definition 2.8 *A* topological ring *R is a ring together with a topology on its underlying set such that R forms a topological group under its addition, and the multiplication law $R \times R \longrightarrow R$ is continuous.*

Let $(R, \mathfrak{m})$ be a local noetherian ring. There is a natural topology on R, called the $\mathfrak{m}$-*adic topology*, obtained by taking $\{\mathfrak{m}^n\}_{n\in\mathbb{N}}$ to be a fundamental system of neighbourhoods of 0 (and thus defining a fundamental system of neighbourhoods of each point by translation). This topology gives $(R, \mathfrak{m})$ the structure of a topological ring. Since R is noetherian, $\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = \{0\}$ (see [Lan93], Ch. X, Corollary 5.7); thus the $\mathfrak{m}$-adic topology is Hausdorff. This topology is precisely that obtained from the metric d on $(R, \mathfrak{m})$ given by

$$d(r,s) = \begin{cases} 0 & \text{if } r = s \\ e^{-v(r-s)} & \text{otherwise} \end{cases} \tag{2.9}$$

where $v : R \setminus \{0\} \longrightarrow \mathbb{N}$, called the $\mathfrak{m}$-*adic valuation* on R, is given by $v(r) = \max\{n \in \mathbb{N} : r \in \mathfrak{m}^n\}$. Thus we may consider Cauchy sequences and convergence in R. We say that $(R, \mathfrak{m})$ is *complete* if R is complete with respect to the metric d.

Proposition 2.10 *Given $(R, \mathfrak{m})$ as above, there exists a complete local ring $(\hat{R}, \hat{\mathfrak{m}})$ together with a continuous injective homomorphism $\phi : R \longrightarrow \hat{R}$ satisfying the following universal property: given any complete local ring $(A, \mathfrak{n})$ together with a continuous homomorphism $\psi : R \longrightarrow A$, there is a unique continuous homomorphism $\hat{\psi} : \hat{R} \longrightarrow A$ such that*

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[dr, "\psi"'] & \hat{R} \arrow[d, "\hat{\psi}"] \\ & A \end{tikzcd}$$

commutes.

Proof: See [GS71], §2. $\square$

The completion $\hat{R}$ of R may be identified with $\varprojlim_{n \in \mathbb{N}} R/\mathfrak{m}^n$, where the inverse limit is taken with respect to the canonical maps. In this case, ϕ is the natural injection $R \longrightarrow \hat{R}$. Moreover, $\hat{\mathfrak{m}}$ is the ideal generated by $\phi(\mathfrak{m})$ and R is itself complete if and only if ϕ is an isomorphism. For details, see [GS71], §2.

Example 2.11 Let R be the localization of $\mathbb{Z}$ at a prime ideal (p), so that (R, pR) is a local ring. The completion of (R, pR), denoted $\mathbb{Z}_p$, is called the ring of *p-adic integers*. By the above remark, $\mathbb{Z}_p$ is isomorphic to $\varprojlim_{n \in \mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$. The quotient field $\mathbb{Q}_p$ of $\mathbb{Z}_p$ is called the field of *p-adic numbers*.

Example 2.12 Let $k = \mathbb{F}_{p^n}$ denote the finite field of order p^n. The ring $W(k)$ of *Witt vectors over k* is the integral closure of $\mathbb{Z}_p$ in the splitting field of $x^{p^n} - x$ over $\mathbb{Q}_p$. The ring $W(k)$ is a complete local ring with residue field k. In particular, $W(\mathbb{F}_p)$ is equal to $\mathbb{Z}_p$, and if p is odd, $W(\mathbb{F}_{p^2})$ is equal to $\mathbb{Z}_p[\sqrt{\alpha}]$, where $\alpha \in \mathbb{Z}_p^\times$ is not a square in $\mathbb{Z}_p$. See [Ser68], Ch. II, §6 for details.

Example 2.13 Let $(A, \mathfrak{m}_A)$ be a complete noetherian local ring, and let R be the localization of $A[t_1, \dots, t_n]$ at the maximal ideal $\mathfrak{m} := (\mathfrak{m}_A, t_1, \dots, t_n)$. The completion of $(R, \mathfrak{m}R)$ is isomorphic to the ring $A[[t_1, \dots, t_n]]$ of formal power series in n variables with coefficients in A.

Proposition 2.14 *Let R be a noetherian ring. Then the ring $R[[t_1, \dots, t_n]]$ is also noetherian.*

Proof: See [Lan93], Ch. IV, Theorem 9.5 and its Corollary. $\square$

Theorem 2.15 (Hensel's Lemma) *Let $(R, \mathfrak{m})$ be a complete local noetherian ring with residue field k, and let $f(x) \in R[x]$ be a monic polynomial. Suppose that $a \in k$ is a nonrepeated root of the reduction of $f(x) \bmod \mathfrak{m}$. Then $f(x)$ has a unique root $\alpha \in R$ such that α reduces to $a \bmod \mathfrak{m}$.*

Proof: See [Lan93], Ch. XII, Corollary 7.4. $\square$

2.4 Deformation Theory

Fix a prime p. Let Π be a group having the property that its pro-p completion is topologically finitely generated. Let k be a finite field of characteristic p, and fix an absolutely irreducible continuous representation $\bar{\rho} : \Pi \longrightarrow \mathrm{GL}_n(k)$, which will be called the *residual representation*. Let $(R, \mathfrak{m})$ be a complete local noetherian $W(k)$-algebra with residue field k, where $W(k)$ is the ring of Witt vectors of k. A *lift* of $\bar{\rho}$ to R is a continuous homomorphism $\rho : \Pi \longrightarrow \mathrm{GL}_n(R)$ such that the diagram

$$\begin{tikzcd} \Pi \arrow[r, "\rho"] \arrow[dr, "\bar{\rho}"'] & \mathrm{GL}_n(R) \arrow[d, "r"] \\ & \mathrm{GL}_n(k) \end{tikzcd}$$

commutes, where r is the map which takes a matrix to its entrywise reduction mod $\mathfrak{m}$. We define an equivalence relation $\sim$, called *strict equivalence*, on the set of lifts of $\bar{\rho}$ to R by $\rho_1 \sim \rho_2$ if there exists an $M \in \mathrm{GL}_n^\circ(R) := \ker(r)$ satisfying $\rho_1 = M\rho_2 M^{-1}$ (that is, $\rho_1(\gamma) = M\rho_2(\gamma)M^{-1}$ for all $\gamma \in \Pi$). A *deformation* of $\bar{\rho}$ to R is a strict equivalence class $[\rho]$ of lifts of $\bar{\rho}$ to R. Note that $[\bar{\rho}] = \{\bar{\rho}\}$ and whenever $M \in \mathrm{GL}_n^\circ(R)$, conjugating a lift ρ of $\bar{\rho}$ by M gives another lift of $\bar{\rho}$. We will often write ρ in place of $[\rho]$ when there is no risk of confusion.

Define a category $\mathcal{DEF}(\bar{\rho})$ whose objects are pairs $(R, [\rho])$, where R is a complete local noetherian $W(k)$-algebra with residue field k, and $[\rho]$ is a deformation of $\bar{\rho}$ to R. A morphism from $(R_1, [\rho_1])$ to $(R_2, [\rho_2])$ in $\mathcal{DEF}(\bar{\rho})$ is a continuous homomorphism $\phi : R_1 \longrightarrow R_2$ reducing to the identity on k, such that for some $\rho_2' \in [\rho_2]$, the diagram

$$\begin{tikzcd} \Pi \arrow[r, "\rho_1"] \arrow[dr, "\rho_2'"'] & \mathrm{GL}_n(R_1) \arrow[d, "\tilde{\phi}"] \\ & \mathrm{GL}_n(R_2) \end{tikzcd}$$

commutes, where $\tilde{\phi}$ denotes the map obtained by applying ϕ entrywise to a given matrix. Using a result of Schlessinger which guarantees the representability of functors satisfying certain criteria, Mazur proved the following theorem:

Theorem 2.16 (Mazur, 1989) *There exists a universal element in the category $\mathcal{DEF}(\bar{\rho})$; that is, there exists a pair $(R^{\mathrm{univ}}, \rho^{\mathrm{univ}}) \in \mathcal{DEF}(\bar{\rho})$ such that for each $(R, \rho) \in \mathcal{DEF}(\bar{\rho})$, there is a unique $\phi : R^{\mathrm{univ}} \longrightarrow R$ such that $\phi \in \mathrm{Mor}\,(\mathcal{DEF}(\bar{\rho}))$.*

Proof: See [Maz89], §1.2. □

As usual, $(R^{\mathrm{univ}}, \rho^{\mathrm{univ}})$ is well-defined up to unique isomorphism in the category $\mathcal{DEF}(\bar{\rho})$. We call ρ^{univ} the *universal deformation* of $\bar{\rho}$. In [dL97], Lenstra and de Smit give an explicit construction of R^{univ} in terms of generators and relations; however, their construction requires many more generators than are usually necessary, and is not very practical when considering specific examples. In what follows, we will consider only the cases $k = \mathbb{F}_p$ or $\mathbb{F}_{p^2}$ and $n = 2$.

Proposition 2.17 *Let $\bar{\rho}$ be a residual representation, and $(R^{\mathrm{univ}}, \rho^{\mathrm{univ}})$ its universal deformation. Then the entries of the elements of* $\mathrm{Im}\rho^{\mathrm{univ}}$ *topologically generate R^{univ}.*

Proof: Let S denote the complete subring of R^{univ} (topologically) generated by the entries of the elements of $\mathrm{Im}\rho^{\mathrm{univ}}$. Then ρ^{univ} maps to S, so the universal property of R^{univ} gives a morphism $\iota : R^{\mathrm{univ}} \longrightarrow S$ in $\mathcal{DEF}(\bar{\rho})$. By the definition of S, ι is surjective. Given $(A, \rho) \in \mathcal{DEF}(\bar{\rho})$, the universal property of R^{univ} gives a morphism $\tau : R^{\mathrm{univ}} \longrightarrow A$ in $\mathcal{DEF}(\bar{\rho})$, which restricts a morphism on S. On the other hand, if $\tau_1, \tau_2 : S \longrightarrow A$ are two such morphisms, then $\tau_1 \circ \iota, \tau_2 \circ \iota : R^{\mathrm{univ}} \longrightarrow A$ are two such morphisms, and hence are equal. Since ι is surjective, it follows that τ_1 is equal to τ_2, and therefore $(S, \rho^{\mathrm{univ}})$ is universal in $\mathcal{DEF}(\bar{\rho})$, and ι is an isomorphism. □

Let $(R, \mathfrak{m}_R)$ be a local noetherian $W(k)$-algebra.

Definition 2.18 *The* (Zariski) cotangent space *of R is the k-vector space $t_R^* := \mathfrak{m}_R/(p, \mathfrak{m}_R^2)$. The* (Zariski) tangent space t_R *of R is the dual space* $\mathrm{Hom}_k(t_R^*, k)$ *of the cotangent space of R.*

Note that since R is noetherian, t_R^* and t_R are finite-dimensional vector spaces, and hence are abstractly isomorphic.

Proposition 2.19 *Let R and S be local noetherian $W(k)$-algebras, and let $f : R \longrightarrow S$ be a $W(k)$-algebra homomorphism reducing to the identity on k. Then f induces a k-linear map $f_* : t_R^* \longrightarrow t_S^*$ which is surjective if and only if f is surjective.*

Proof: For each $m \in \mathfrak{m}_R$, $f(m) \in \mathfrak{m}_S$, so f restricts to an additive homomorphism $\bar{f} : \mathfrak{m}_R \longrightarrow \mathfrak{m}_S/(p, \mathfrak{m}_S^2)$. Checking that $\bar{f}(p, \mathfrak{m}_R^2) = 0$, we obtain a k-linear map $f_* : t_R^* \longrightarrow t_S^*$.

Suppose now that f is surjective. Then $\bar{f} : R \longrightarrow S/(p, \mathfrak{m}_S^2)$ is surjective, and hence $\bar{f}(\mathfrak{m}_R) = \mathfrak{m}_S/(p, \mathfrak{m}_S^2)$. Thus f_* is surjective.

Conversely, suppose that f_* is surjective. The reduction of $f \mod p$ makes $\mathfrak{m}_S/p\mathfrak{m}_S$ into an R/pR-module; thus f gives rise to an R/pR-module homomorphism $f^+ : \mathfrak{m}_R/p\mathfrak{m}_R \longrightarrow \mathfrak{m}_S/p\mathfrak{m}_S$, which reduces to a homomorphism $\bar{f}^+ : \mathfrak{m}_R/(p, \mathfrak{m}_R^2) \longrightarrow \mathfrak{m}_S/(p, \mathfrak{m}_R\mathfrak{m}_S)$. Given $\alpha \in \mathfrak{m}_S^2$, write $\alpha = m_1 m_2$ with $m_1, m_2 \in \mathfrak{m}_S, m_1 \notin \mathfrak{m}_S^2$. Since f_* is surjective, there is some $m_1' \in \mathfrak{m}_R$ such that $m_1 = m_1' + \tilde{m}$, where $\tilde{m} \in (p, \mathfrak{m}_S^2)$, and hence $\alpha = (m_1' + \tilde{m})m_2$. Thus we have shown that

$$\mathfrak{m}_S^2/p\mathfrak{m}_S^2 \subset (\mathfrak{m}_R/p\mathfrak{m}_R)\mathfrak{m}_S/p\mathfrak{m}_S + \mathfrak{m}_S^3/p\mathfrak{m}_S^3.$$

By induction,

$$\mathfrak{m}_S^2/p\mathfrak{m}_S^2 \subset (\mathfrak{m}_R/p\mathfrak{m}_R)\mathfrak{m}_S/p\mathfrak{m}_S + \mathfrak{m}_S^n/p\mathfrak{m}_S^n$$

for all n, which implies that $\mathfrak{m}_S^2/p\mathfrak{m}_S^2 = (\mathfrak{m}_R/p\mathfrak{m}_R)\mathfrak{m}_S/p\mathfrak{m}_S$ since S is noetherian. Thus $\bar{f}^+$ is surjective, and by a corollary of Nakayama's lemma, f^+ is itself surjective (see [Lan93], Ch. X, Proposition 4.5). Viewing $\mathfrak{m}_R$ and $\mathfrak{m}_S$ as $W(k)$-modules and applying Nakayama's lemma shows that $f(\mathfrak{m}_R) = \mathfrak{m}_S$. Every element of S can be expressed as $\lambda + m$ with $\lambda \in W(k)$ and $m \in \mathfrak{m}_S$, so this proves that f is surjective since $f(W(k)) = W(k)$. $\square$

2.5 The Universal Deformation

Let K be an algebraic extension of $\mathbb{Q}$. Throughout the sequel, let

$$\Pi := \mathrm{Gal}\left(\widehat{\overline{K}(t)}/\overline{K}(t)\right),$$

where $\widehat{\overline{K}(t)}$ denotes the maximal algebraic extension of $\overline{K}(t)$ unramified outside 0,1, and ∞. Fix a prime p, and let k be a finite field of characteristic p. It follows from Theorem 2.7 that the pro-p completion of Π is topologically finitely generated. Let $\bar{\rho} : \Pi \longrightarrow \mathrm{GL}_2(k)$ be a residual representation.

Proposition 2.20 *The universal deformation ring R^{univ} of $\bar{\rho}$ is isomorphic to a power series ring with coefficients in $W(k)$.*

Proof: By Proposition 2.14 and Examples 2.12 and 2.13 of §2.3, any power series ring $W(k)[[t_1, \dots, t_d]]$ is a complete noetherian local ring. Writing R for R^{univ}, let d denote the k-dimension of t_R^*, and let $\bar{x}_1, \dots, \bar{x}_d \in t_R^*$ be a collection of elements which forms a basis for t_R^*. Choose lifts $x_1, \dots, x_d \in \mathfrak{m}_R$ of $\bar{x}_1, \dots, \bar{x}_d$ respectively. Defining $\phi(t_i) = x_i$ for each $i = 1, \dots, d$ gives rise to a continuous $W(k)$-algebra homomorphism $\phi : W(k)[[t_1, \dots, t_d]] \longrightarrow R$ which reduces to the identity on k. Since the reductions $\bar{t}_1, \dots, \bar{t}_d$ of $t_1, \dots, t_d$ mod $(p, \mathfrak{m}_{W(k)[[t_1,\dots,t_d]]})$ form a basis for $t^*_{W(k)[[t_1,\dots,t_d]]}$, and $\phi_*(\bar{t}_i) = \bar{x}_i$ for each i, ϕ_* is a k-vector space isomorphism. In particular, ϕ_* is surjective, and therefore, by Lemma 2.19, ϕ is itself surjective.

Fix elements σ_0, σ_1 of Π which generate Π topologically, and choose for each $i = 0, 1$ a lift $M_i \in \tilde{\phi}^{-1}\left(\rho^{\mathrm{univ}}(\sigma_i)\right)$ of $\rho^{\mathrm{univ}}(\sigma_i)$, where $\tilde{\phi}$ denotes the map induced from ϕ. We obtain a deformation $\rho : \Pi \longrightarrow \mathrm{GL}_2(W(k)[[t_1, \dots, t_d]])$ such that $\rho(\sigma_i) = M_i$ for $i = 0, 1$, and $\tilde{\phi} \circ \rho = \rho^{\mathrm{univ}}$. By the universal property of R, there is a map $\psi : R \longrightarrow W(k)[[t_1, \dots, t_d]]$ such that $\rho = \tilde{\psi} \circ \rho^{\mathrm{univ}}$. We claim that ψ splits ϕ, that is, $\phi \circ \psi = \mathrm{Id}_R$. Given $M \in \mathrm{Im}\rho^{\mathrm{univ}}$, let $\sigma \in \Pi$ be a preimage of M; then

$$\tilde{\phi} \circ \tilde{\psi}(M) = \tilde{\phi} \circ \tilde{\psi}(\rho^{\mathrm{univ}}(\sigma)) = \tilde{\phi}(\rho(\sigma)) = \rho^{\mathrm{univ}}(\sigma),$$

so if $r \in R$ is an entry of some $M \in \mathrm{Im}\rho^{\mathrm{univ}}$, then $\phi \circ \psi(r) = r$. Applying Proposition 2.17 proves the claim. Now $\phi \circ \psi = \mathrm{Id}_R$ implies that $\phi_* \circ \psi_* = \mathrm{Id}_{t_R^*}$, so ψ_* is an isomorphism. In particular, ψ is surjective. Therefore, ψ is an isomorphism, as desired. $\square$

If Π were to be replaced with some other profinite group in Proposition 2.20, it would not necessarily be possible to lift ρ^{univ} to $W(k)[[t_1, \dots, t_d]]$. However, the proof that we have given works with only minor changes provided that the cohomology group $H^2(\Pi, \mathrm{ad}(\bar{\rho}))$ is trivial, where $\mathrm{ad}(\bar{\rho})$ denotes the matrix ring $\mathrm{M}_2(k)$ together with the action of Π given by

$$\sigma \cdot M = \bar{\rho}(\sigma) M \bar{\rho}(\sigma)^{-1}$$

for each $\sigma \in \Pi$, $M \in \mathrm{M}_2(k)$. Mazur showed moreover that the Krull dimension of $R^{\mathrm{univ}}/pR^{\mathrm{univ}}$ is at least $d_1 - d_2$, where $d_i = \dim_k H^i(\Pi, \mathrm{ad}(\bar{\rho}))$, with equality when $d_2 = 0$ (see [Maz89], §1.6 and [Gou], p.50 for details). As we shall see, $H^1(\Pi, \mathrm{ad}(\bar{\rho}))$ is naturally isomorphic to $t_{R^{\mathrm{univ}}}$ (as a k-vector space), so Mazur's result agrees with the choice of d in the proof of Proposition 2.20.

Fix a residual representation

$$\bar{\rho} : \Pi \longrightarrow \mathrm{GL}_2(\mathbb{F}_p).$$

In order to determine $R^{\mathrm{univ}}(\bar{\rho})$ explicitly, it may be convenient to extend scalars to $\mathbb{F}_{p^2}$, and thus replace $\bar{\rho}$ with $\bar{\rho}'$, where $\bar{\rho}'$ is obtained by composing $\bar{\rho}$ with the inclusion $\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^2}$. Let R' be the universal deformation ring corresponding to $\bar{\rho}'$; by Proposition 2.20, $R' = W(\mathbb{F}_{p^2})[[t_1, \ldots, t_{d'}]]$ for some d'. We will show that $R^{\mathrm{univ}} = \mathbb{Z}_p[[t_1, \ldots, t_{d'}]]$, so that R^{univ} may be recovered from R'. By Proposition 2.20, $R^{\mathrm{univ}} = \mathbb{Z}_p[[t_1, \ldots, t_d]]$ for some d, so it suffices to show that $d = d'$. If we show that for any residual representation $\bar{\varrho} : G \longrightarrow \mathrm{GL}_2(k)$, there is a k-vector space isomorphism

$$t_{R^{\mathrm{univ}}(\bar{\varrho})} \cong H^1(G, \mathrm{ad}(\bar{\varrho})),$$

then we have

$$\begin{aligned} d' &= \dim_{\mathbb{F}_{p^2}} H^1(\Pi, \mathrm{ad}(\bar{\rho}')) \\ &= \dim_{\mathbb{F}_{p^2}} H^1(\Pi, \mathrm{ad}(\bar{\rho}) \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}) \\ &= \dim_{\mathbb{F}_{p^2}} H^1(\Pi, \mathrm{ad}(\bar{\rho})) \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2} \\ &= \dim_{\mathbb{F}_p} H^1(\Pi, \mathrm{ad}(\bar{\rho})) = d, \end{aligned}$$

as desired.

Let $(R^{\mathrm{univ}}, \varrho^{\mathrm{univ}})$ be the universal deformation of a residual representation $\bar{\varrho} : G \longrightarrow \mathrm{GL}_2(k)$. The isomorphism $t_{R^{\mathrm{univ}}} \cong H^1(G, \mathrm{ad}(\bar{\varrho}))$ arises naturally through deformations of $\bar{\varrho}$ to the ring of *dual numbers* $k[\epsilon]$, where $\epsilon^2 = 0$. First, there is a k-vector space isomorphism $t_{R^{\mathrm{univ}}} \cong \mathrm{Hom}_{W(k)}(R^{\mathrm{univ}}, k[\epsilon])$, where $\mathrm{Hom}_{W(k)}(R^{\mathrm{univ}}, k[\epsilon])$ consists of continuous $W(k)$-algebra homomorphisms reducing to the identity on k. Given $\phi \in \mathrm{Hom}_{W(k)}(R^{\mathrm{univ}}, k[\epsilon])$, and $r \in R^{\mathrm{univ}}$, let $\bar{r} \in k$ denote the reduction of $r \mod \mathfrak{m}_{R^{\mathrm{univ}}}$; since ϕ reduces to the identity on k, there is some $\phi'(r) \in k$ for which $\phi(r) = \bar{r} + \phi'(r)\epsilon$. Restricting ϕ' to $\mathfrak{m}_{R^{\mathrm{univ}}}$ gives an additive homomorphism whose kernel contains $(p, \mathfrak{m}^2_{R^{\mathrm{univ}}})$, and thus $\phi'|_{\mathfrak{m}_{R^{\mathrm{univ}}}}$ factors through a map $\phi'^* : t^*_{R^{\mathrm{univ}}} \longrightarrow k$ which is k-linear since ϕ is $W(k)$-linear. Furthermore, since ϕ is a $W(k)$-algebra homomorphism, it is completely determined by $\phi'|_{\mathfrak{m}_{R^{\mathrm{univ}}}}$, so the correspondence $\phi \longleftrightarrow \phi'^*$ defines a bijection $\mathrm{Hom}_{W(k)}(R^{\mathrm{univ}}, k[\epsilon]) \longleftrightarrow t_{R^{\mathrm{univ}}}$ which is k-linear.

On the other hand, there is a natural k-vector space isomorphism

$$\mathrm{Hom}_{W(k)}(R^{\mathrm{univ}}, k[\epsilon]) \cong H^1(G, \mathrm{ad}(\bar{\varrho})). \tag{2.21}$$

First, there is a bijective correspondence between $\mathrm{Hom}_{W(k)}(R^{\mathrm{univ}}, k[\epsilon])$ and the set of deformations of $\bar{\rho}$ to $k[\epsilon]$, given by $\phi \longleftrightarrow \tilde{\phi} \circ \rho^{\mathrm{univ}}$. For any lift $\varrho : G \longrightarrow \mathrm{GL}_2(k[\epsilon])$ of $\bar{\varrho}$, let $\varrho' : G \longrightarrow \mathrm{M}_2(k)$ denote the set-theoretic map satisfying

$$\varrho(g) = \bar{\varrho}(g)(1 + \varrho'(g)\epsilon)$$

for all $g \in G$. Then ϱ' is a 1-cocycle with values in $\mathrm{ad}(\bar{\varrho})$, and a lift ϱ_1 of $\bar{\varrho}$ is strictly equivalent to ϱ if and only if ϱ_1' differs from ϱ' by a coboundary. Thus deformations of $\bar{\varrho}$ to $k[\epsilon]$ correspond to elements of $H^1(G, \mathrm{ad}(\bar{\varrho}))$; in fact, this correspondence defines the desired k-vector space isomorphism $\mathrm{Hom}_{W(k)}(R^{\mathrm{univ}}, k[\epsilon]) \cong H^1(G, \mathrm{ad}(\bar{\varrho}))$, and therefore gives rise to the isomorphism $t_{R^{\mathrm{univ}}} \cong H^1(G, \mathrm{ad}(\bar{\rho}))$. In particular, when $G = \Pi$ and $\bar{\rho} = \bar{\varrho}$, we may conclude that if $R' = W(\mathbb{F}_{p^2})[[t_1, \ldots , t_d]]$, then $R^{\mathrm{univ}} = \mathbb{Z}_p[[t_1, \ldots , t_d]]$.

To determine the value of d, we will single out a distinguished representative for each deformation $[\rho]$ of $\bar{\rho}$. We will need the following lemma:

Lemma 2.22 *Suppose that $p > 3$. Then there exist elements $\sigma_0, \sigma_1 \in \Pi$ such that σ_0, σ_1 topologically generate Π, and $\bar{\rho}(\sigma_0), \bar{\rho}(\sigma_1)$ each have distinct eigenvalues in $\mathbb{F}_{p^2}$.*

Proof: Let $\gamma_0, \gamma_1 \in \Pi$ be any two elements which (topologically) generate Π. Extending scalars to $\mathbb{F}_{p^2}$, the matrices $\bar{\rho}(\gamma_0)$, $\bar{\rho}(\gamma_1)$ have eigenvectors $\mathbf{v}_0$, $\mathbf{v}_1$ respectively. Since $\bar{\rho}$ is absolutely irreducible, $\mathbf{v}_0$, $\mathbf{v}_1$ form a basis for $\mathbb{F}_{p^2}^2$, and writing $\bar{\rho}(\gamma_0)$, $\bar{\rho}(\gamma_1)$ with respect to this basis gives $\bar{\rho}(\gamma_0) = \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ and $\bar{\rho}(\gamma_1) = \left(\begin{smallmatrix} d & 0 \\ f & g \end{smallmatrix}\right)$, for some $a, b, c, d, f, g \in \mathbb{F}_{p^2}$. Since $\bar{\rho}$ is absolutely irreducible, b and f are both nonzero. Rescaling $\mathbf{v}_0, \mathbf{v}_1$ (equivalently, conjugating by an appropriate diagonal matrix), we may assume that $b = 1$. Suppose first that only one of $\bar{\rho}(\gamma_0)$ or $\bar{\rho}(\gamma_1)$ has distinct eigenvalues. Then without loss of generality, we have $d \neq g$. Now $\bar{\rho}(\gamma_0\gamma_1)$ has characteristic polynomial

$$f(X) = X^2 - (ad + f + ag)X + a^2dg,$$

which has a repeated root if and only if $\left(\frac{ad+f+ag}{2}\right)^2 = a^2dg$ (since $p \neq 2$). Similarly, $\bar{\rho}(\gamma_0\gamma_1^{-1})$ has a repeated eigenvalue if and only if $\left(\frac{ad+ag-f}{2}\right)^2 = a^2dg$. In particular, if both $\bar{\rho}(\gamma_0\gamma_1)$ and $\bar{\rho}(\gamma_0\gamma_1^{-1})$ have repeated eigenvalues, then $(ad + ag - f)^2 = (ad + f + ag)^2$; expanding gives $d = -g$ since $a \neq 0$ and $f \neq 0$. Also, the equalities $\left(\frac{ad+f+ag}{2}\right)^2 = a^2dg$ and $d = -g$ imply that $f^2 = -4a^2d^2$. If $\bar{\rho}(\gamma_0\gamma_1)$ and $\bar{\rho}(\gamma_0\gamma_1^{-1})$ both have repeated eigenvalues, then a similar calculation shows that $\bar{\rho}(\gamma_0^2\gamma_1)$ has a repeated eigenvalue if and only if $f^2 = -a^2d^2$, which is impossible when $p \neq 3$ since $f^2 = -4a^2d^2$, $a \neq 0$ and $d \neq 0$. Similarly, $\bar{\rho}(\gamma_0^3\gamma_1)$ has a repeated eigenvalue if and only if $9f^2 = -4a^2d^2$, which is impossible when $p \neq 2$ since $f^2 = -4a^2d^2$. Therefore, at least one of the pairs $(\gamma_0\gamma_1, \gamma_1)$, $(\gamma_0\gamma_1^{-1}, \gamma_1)$, or $(\gamma_0^2\gamma_1, \gamma_0^3\gamma_1)$ gives the desired (σ_0, σ_1).

Suppose now that $\bar{\rho}(\gamma_0)$, $\bar{\rho}(\gamma_1)$ both have repeated eigenvalues. Without loss of generality, we may assume that $\bar{\rho}(\gamma_0) = \left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ and $\bar{\rho}(\gamma_1) = \left(\begin{smallmatrix} b & 0 \\ c & b \end{smallmatrix}\right)$, for some $a, b, c \in \mathbb{F}_{p^2}^\times$. A simple calculation shows that $\bar{\rho}(\gamma_0\gamma_1)$ has a repeated eigenvalue if and only if $4ab + c = 0$. Similarly, $\bar{\rho}(\gamma_1\gamma_0\gamma_1)$ has a repeated eigenvalue if and only if $2ab + c = 0$, which cannot be the case when $p \neq 2$ if $\bar{\rho}(\gamma_0\gamma_1)$ has a repeated eigenvalue. Therefore at least one of the pairs $(\gamma_0\gamma_1, \gamma_1)$ or $(\gamma_1\gamma_0\gamma_1, \gamma_1)$ generates Π and has the property that the image of its first component has distinct eigenvalues. This reduces the problem to the case considered above, thus proving the lemma. $\square$

Let F be a free module over a ring R, and M an endomorphism of F.

Definition 2.23 *An element* $\mathbf{v} \in F$ *is said to be an* eigenvector *of* M *(with eigenvalue* λ*) if there exists some* $\lambda \in R$ *satisfying* $M\mathbf{v} = \lambda\mathbf{v}$, *and* $\mathbf{v}$ *may be completed to a basis of* F.

Remark: If R is a local ring, and F is finitely generated over R, then by Nakayama's lemma, $\mathbf{v} \in F$ may be completed to a basis of F if and only if the reduction of $\mathbf{v} \mod \mathfrak{m}_R$ is nontrivial.

Proposition 2.24 *Let* $(R, \mathfrak{m})$ *be a local ring with residue field* k. *Suppose that* $M \in \mathrm{GL}_2(R)$ *does not reduce to a scalar matrix* $\mathrm{mod}\ \mathfrak{m}$. *Then* M *has an eigenvector in* R^2 *with eigenvalue* $\lambda \in R$ *if and only if* λ *is a root of the characteristic polynomial* $\mathrm{ch}(M)$ *of* M.

Proof: Let $\bar{M}$ denote the reduction of $M \mod \mathfrak{m}$. Since $\bar{M}$ is not a scalar matrix, there is a basis $\{\bar{\mathbf{b}}_1, \bar{\mathbf{b}}_2\}$ of k^2 with respect to which $\bar{M}$ has at least three nonzero entries. Let $\mathbf{b}_1, \mathbf{b}_2 \in R^2$ be elements reducing to $\bar{\mathbf{b}}_1, \bar{\mathbf{b}}_2 \mod \mathfrak{m}$. By Nakayama's lemma, $\{\mathbf{b}_1, \mathbf{b}_2\}$ forms a basis for R^2. Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with respect to $\{\mathbf{b}_1, \mathbf{b}_2\}$. Assume that $a, b, d \in R^\times$ (if not, one may apply a similar argument using the three entries of M which are units). Suppose that $\lambda \in R$ is a root of $\mathrm{ch}(M)$. Then we claim that $\mathbf{v} = \mathbf{b}_1 + (\frac{\lambda - a}{b})\mathbf{b}_2$ is an eigenvector of M having eigenvalue λ. Clearly $\mathbf{v}$ reduces to a nontrivial vector mod $\mathfrak{m}$. Expanding gives $M\mathbf{v} = \lambda\mathbf{b}_1 + \left(c + d(\frac{\lambda - a}{b})\right)\mathbf{b}_2$. Since λ is a root of $\mathrm{ch}(M)$, we have $(a - \lambda)(d - \lambda) - bc = 0$, and hence $\lambda(\frac{\lambda - a}{b}) = c + d(\frac{\lambda - a}{b})$. Substituting into the above expression for $M\mathbf{v}$ proves the claim.

Conversely, suppose that $\mathbf{v} \in R^2$ is an eigenvector of M with eigenvalue $\lambda \in R$. By Nakayama's lemma, there is a vector $\mathbf{v}' \in R^2$ such that $\{\mathbf{v}, \mathbf{v}'\}$ forms a basis for R^2. With respect to this basis, $M = \left(\begin{smallmatrix} \lambda & b \\ 0 & d \end{smallmatrix}\right)$ for some $b, d \in R$. Thus $\mathrm{ch}(M) = (X - \lambda)(X - d)$, so λ is indeed a root of $\mathrm{ch}(M)$. $\square$

Conjugating $\bar{\rho}$ only affects ρ^{univ} by conjugation, for if $M \in \mathrm{GL}_2(\mathbb{F}_p)$, then choosing any lift $\tilde{M} \in \mathrm{GL}_2(R^{\mathrm{univ}})$ of M, the deformation $(R^{\mathrm{univ}}, \tilde{M}\rho^{\mathrm{univ}}\tilde{M}^{-1})$ is the universal deformation of $M\bar{\rho}M^{-1}$. Thus in order to determine R^{univ}, we are free to alter $\bar{\rho}$ by changing to any basis of $\mathbb{F}_p^2$. Let σ_0, σ_1 be as in Lemma 2.22; since σ_0, σ_1 topologically generate Π, the residual representation $\bar{\rho}$ is completely determined by $\bar{\rho}(\sigma_0), \bar{\rho}(\sigma_1)$. Extending scalars to $\mathbb{F}_{p^2}$, we may assume (as in the proof of Lemma 2.22) that $\bar{\rho}(\sigma_0) = \left(\begin{smallmatrix} a_0 & 1 \\ 0 & d_0 \end{smallmatrix}\right)$ and $\bar{\rho}(\sigma_1) = \left(\begin{smallmatrix} a_1 & 0 \\ c_1 & d_1 \end{smallmatrix}\right)$ for some $a_0, d_0, a_1, c_1, d_1 \in \mathbb{F}_{p^2}^\times$ satisfying $a_0 \neq d_0$ and $a_1 \neq d_1$. Fix lifts $\alpha_0, \delta_0, \alpha_1, \eta_1, \delta_1$ of a_0, d_0, a_1, c_1, d_1 respectively to $W(\mathbb{F}_{p^2})$. The following lemma will suggest a candidate for ρ^{univ}:

Lemma 2.25 *Let $(A, [\rho])$ be a deformation of $\bar{\rho} \otimes \mathbb{F}_{p^2}$. Then there is a unique representative $\rho_g \in [\rho]$ for which there exist $m_0, m_1, n_0, n_1, n_2 \in \mathfrak{m}_A$ such that*

$$\rho_g(\sigma_0) = \begin{pmatrix} \alpha_0(1 + m_0) & 1 \\ 0 & \delta_0(1 + m_1) \end{pmatrix}$$

$$\textit{and} \qquad \rho_g(\sigma_1) = \begin{pmatrix} \alpha_1(1 + n_0) & 0 \\ \eta_1(1 + n_1) & \delta_1(1 + n_2) \end{pmatrix}.$$

Proof: Let $f(x)$ be the characteristic polynomial of $\rho(\sigma_0)$. Since the roots a_0, d_0 of the reduction $\bar{f}(x)$ of $f(x) \mod \mathfrak{m}_A$ are distinct, $f(x)$ satisfies the hypotheses of Hensel's lemma, and therefore has a root $\lambda_0 \in A$ reducing to

$a_0 \mod \mathfrak{m}_A$. By Proposition 2.24, $\rho(\sigma_0)$ has an eigenvector $\mathbf{x}_0 \in A^2$ with eigenvalue λ_0. Similarly, $\rho(\sigma_1)$ has an eigenvector $\mathbf{x}_1 \in A^2$ with eigenvalue $\lambda_1 \in A$ such that λ_1 reduces to $d_1 \mod \mathfrak{m}_A$. Since $\bar{\rho}$ is absolutely irreducible, the reductions $\bar{\mathbf{x}}_0, \bar{\mathbf{x}}_1$ of $\mathbf{x}_0, \mathbf{x}_1 \mod \mathfrak{m}_A$ are linearly independent; hence by Nakayama's lemma, $\{\mathbf{x}_0, \mathbf{x}_1\}$ forms a basis for M. Let $\rho_g : \Pi \longrightarrow \mathrm{GL}_2(A)$ denote the homomorphism obtained by writing ρ with respect to this basis, so that $\rho_g(\sigma_0)$ is upper-triangular and $\rho_g(\sigma_1)$ is lower-triangular. Rescaling $\{\mathbf{x}_0, \mathbf{x}_1\}$ if necessary, we may assume that $\rho_g(\sigma_0) = \left(\begin{smallmatrix} * & 1 \\ 0 & * \end{smallmatrix}\right)$. Since λ_0 reduces to a_0 and λ_1 reduces to d_1, and since ρ_g is conjugate to ρ, the reduction of $\rho_g \mod \mathfrak{m}_A$ is equal to $\bar{\rho}$. Let $B \in \mathrm{GL}_2(A)$ be such that $\rho_g = B\rho B^{-1}$. Since $\bar{\rho}$ is absolutely irreducible, Schur's lemma together with the fact that $\bar{\rho}_g = \bar{\rho}$ imply that B must reduce to a scalar matrix mod $\mathfrak{m}$. Multiplying B by an appropriate scalar thus gives $B \in \mathrm{GL}_2^\circ(A)$, so $\rho_g \in [\rho]$. This proves the existence of ρ_g.

To prove uniqueness, suppose $\rho' \in [\rho_g]$ is also of the given form. Let $b_0, b_1, b_2, b_3 \in \mathfrak{m}$ be such that $B = \left(\begin{smallmatrix} 1+b_0 & b_1 \\ b_2 & 1+b_3 \end{smallmatrix}\right)$ satisfies $\rho' = B\rho_g B^{-1}$. In particular, we have

$$\begin{aligned} \rho'(\sigma_0) &= B\rho_g(\sigma_0)B^{-1} \\ &= \frac{1}{\det B}\left(\begin{smallmatrix} * & (1+b_0)((1+b_0)-\alpha_0(1+m_0)b_1+b_1\delta_0(1+m_1)) \\ b_2((\alpha_0-\delta_0)(1+b_3)-b_2) & * \end{smallmatrix}\right). \end{aligned} \tag{2.26}$$

By assumption, the lower-left entry of $\rho'(\sigma_0)$ is zero, that is,

$$b_2((\alpha_0 - \delta_0)(1 + b_3) - b_2) = 0.$$

Since $\alpha_0 - \delta_0$ is a unit, so is $(\alpha_0 - \delta_0)(1 + b_3) - b_2$, and therefore $b_2 = 0$. Applying the same argument to the upper-right entry of $\rho'(\sigma_1)$ gives $b_1 = 0$. Putting $b_2 = b_1 = 0$ in (2.26) gives $\rho'(\sigma_0) = \frac{1}{(1+b_0)(1+b_3)} \left(\begin{smallmatrix} * & (1+b_0)^2 \\ 0 & * \end{smallmatrix} \right)$, and hence $\frac{(1+b_0)^2}{(1+b_0)(1+b_3)} = 1$, which implies that $b_0 = b_3$, and therefore $\rho_g = \rho'$. $\square$

Theorem 2.27 *Suppose that $p > 3$ and let $\bar{\rho}$, σ_0, σ_1, α_0, δ_0, α_1, η_1, and δ_1 be as in Lemma 2.25. Then $R^{\mathrm{univ}}(\bar{\rho} \otimes \mathbb{F}_{p^2}) = W(\mathbb{F}_{p^2})[[t_0, t_1, u_0, u_1, u_2]]$, and the corresponding universal deformation ρ^{univ} of $\bar{\rho} \otimes \mathbb{F}_{p^2}$ is conjugate to the deformation ρ given by*

$$\rho(\sigma_0) = \begin{pmatrix} \alpha_0(1 + t_0) & 1 \\ 0 & \delta_0(1 + t_1) \end{pmatrix}, \quad \rho(\sigma_1) = \begin{pmatrix} \alpha_1(1 + u_0) & 0 \\ \eta_1(1 + u_1) & \delta_1(1 + u_2) \end{pmatrix}.$$

Moreover, $R^{\mathrm{univ}}(\bar{\rho}) = \mathbb{Z}_p[[t_1, \ldots, t_5]]$.

Proof: Given any deformation $[\rho]$ of $\bar{\rho} \otimes \mathbb{F}_{p^2}$ to A, choose $\rho_g \in [\rho]$ as in Lemma 2.25. Define a $W(\mathbb{F}_{p^2})$-algebra homomorphism

$$\phi : W(\mathbb{F}_{p^2})[t_0, t_1, u_0, u_1, u_2] \longrightarrow A$$

by $\phi(t_i) = m_i$ and $\phi(u_i) = n_i$ for each i, extended by $W(\mathbb{F}_{p^2})$-linearity. By Proposition 2.10, we may extend ϕ to a continuous homomorphism

$$\phi : W(\mathbb{F}_{p^2})[[t_0, t_1, u_0, u_1, u_2]] \longrightarrow A.$$

In fact, ϕ is a morphism in $\mathcal{DEF}(\bar{\rho} \otimes \mathbb{F}_{p^2})$. To show that ϕ is unique, suppose that $\phi' : W(\mathbb{F}_{p^2})[[t_0, t_1, u_0, u_1, u_2]] \longrightarrow A$ is another such morphism. Letting ϕ' also denote the induced map on the general linear groups, $\phi'(\rho^{\mathrm{univ}}(\sigma_0))$ and

$\phi'(\rho^{\mathrm{univ}}(\sigma_1))$ are of the form given in Lemma 2.25; hence by the uniqueness statement of Lemma 2.25, we have $\phi'(\rho^{\mathrm{univ}}(\sigma_i)) = \rho_g(\sigma_i)$ for $i = 0, 1$. This implies that $\phi(t_i) = \phi'(t_i)$ and $\phi(u_i) = \phi'(u_i)$ for each i, and therefore $\phi = \phi'$, as desired. The final statement now follows from the discussion preceding Lemma 2.22. $\square$

2.6 Conditions on Deformations

If the determinant of a given residual representation $\bar{\rho}$ is 1 (that is, if the image of $\bar{\rho}$ is contained in $\mathrm{SL}_2(k)$), then it is natural to insist that deformations of $\bar{\rho}$ also have determinant 1. Accordingly, let $\mathcal{DEF}^1(\bar{\rho})$ denote the subcategory of $\mathcal{DEF}(\bar{\rho})$ consisting of only those objects $(A, [\rho])$ such that ρ has determinant one. Mazur's proof of the existence of the universal deformation carries over to show that there is a universal object $(R_1^{\mathrm{univ}}, \rho_1^{\mathrm{univ}})$ in $\mathcal{DEF}^1(\bar{\rho})$ (see [Gou], p.68). In fact, imposing a fixed determinant on deformations of $\bar{\rho}$ is perhaps the simplest example of a "deformation condition", that is, a property of deformations which defines a subcategory of $\mathcal{DEF}(\bar{\rho})$ in which a universal object is guaranteed to exist. See [Gou], Lecture 6 for a detailed discussion of such conditions.

Theorem 2.28 *Let notation be as in Theorem* 2.27, *and suppose that* $\bar{\rho}$ *has determinant one. Then* $R_1^{\mathrm{univ}}(\bar{\rho} \otimes \mathbb{F}_{p^2}) = W(\mathbb{F}_{p^2})[[t_0, u_0, u_1]]$, *and the corresponding universal deformation* ρ_1^{univ} *of* $\bar{\rho} \otimes \mathbb{F}_{p^2}$ *is conjugate to the deformation*

ρ_1 given by

$$\rho_1(\sigma_0) = \begin{pmatrix} \alpha_0(1+t_0) & 1 \\ 0 & (\alpha_0(1+t_0))^{-1} \end{pmatrix}$$
$$\text{and} \qquad \rho_1(\sigma_1) = \begin{pmatrix} \alpha_1(1+u_0) & 0 \\ \eta_1(1+u_1) & (\alpha_1(1+u_0))^{-1} \end{pmatrix}.$$

Moreover, $R_1^{\mathrm{univ}}(\bar{\rho}) = \mathbb{Z}_p[[t_1, t_2, t_3]]$.

Proof: If $(A, [\rho]) \in \mathcal{DEF}^1(\bar{\rho} \otimes \mathbb{F}_{p^2})$, then the representative $\rho_g \in [\rho]$ of Lemma 2.25 has determinant one, and hence $\delta_0(1+m_1) = (\alpha_0(1+m_0))^{-1}$, and $\delta_1(1+n_2) = (\alpha_1(1+n_0))^{-1}$. Thus defining $\phi : \mathbb{Z}_p[[t_0, u_0, u_1]] \longrightarrow A$ by $\phi(t_0) = m_0$, $\phi(u_0) = n_0$, and $\phi(u_1) = n_1$ gives a morphism in $\mathcal{DEF}^1(\bar{\rho})$. Uniqueness again follows from the uniqueness of ρ_g.

To obtain $R_1^{\mathrm{univ}}(\bar{\rho})$ from $R_1^{\mathrm{univ}}(\bar{\rho} \otimes \mathbb{F}_{p^2})$, one applies the same argument that was used above for the usual universal deformation, with two minor changes. First, one must choose the lift of ρ^{univ} to $W(k)[[t_1, \dots, t_d]]$ in the proof of Proposition 2.20 to have determinant one. Such a choice is possible since the homomorphism $\phi : W(k)[[t_1, \dots, t_d]] \longrightarrow R^{\mathrm{univ}}$ reduces to the identity on k. Also, one must check that deformations of determinant one correspond to cocycles of trace zero under the isomorphism (2.21). In other words, $t_{R_1^{\mathrm{univ}}} \cong H^1(\Pi, \mathrm{ad}^0(\bar{\rho}))$, where $\mathrm{ad}^0(\bar{\rho})$ is the subgroup of $\mathrm{ad}(\bar{\rho})$ consisting of the trace zero matrices. Thus replacing $H^1(\Pi, \mathrm{ad}(\bar{\rho}))$ with $H^1(\Pi, \mathrm{ad}^0(\bar{\rho}))$, one may apply the above argument to R_1^{univ}, which gives the desired result. $\square$

Given a residual representation $\bar{\rho} : \Pi \longrightarrow \mathrm{GL}_2(k)$, suppose that for some closed subgroup $I \subset \Pi$, the subspace of k^2 consisting of all fixed points of $\bar{\rho}(I)$ has dimension one. A deformation ρ of $\bar{\rho}$ to a ring R is said to be *I-ordinary* if the submodule of R^2 of fixed points of $\rho(I)$ is a direct summand of R^2 of rank one. Note that the condition of being I-ordinary is preserved by strict equivalence, and is therefore a well-defined property of deformations. If $I = \langle \delta \rangle$ for some $\delta \in \Pi$, we will say that ρ is δ-ordinary. By essentially the same argument that he used to prove the existence of the universal deformation, Mazur showed in his original paper [Maz89] that there is a universal I-ordinary deformation whenever $\bar{\rho}$ is itself I-ordinary. If $\bar{\rho}$ has determinant one, then there is a universal I-ordinary deformation of determinant one. Throughout the following, all deformations will be assumed to have determinant one.

Theorem 2.29 *Let σ_0, σ_1 be topological generators of Π. For $p \neq 2$, let $\bar{\rho} : \Pi \longrightarrow \mathrm{SL}_2(\mathbb{F}_p)$ be a residual representation which is σ_i-ordinary for $i = 0$ or $i = 1$. Let $R_{\mathrm{ord}}^{\mathrm{univ}}$ denote the (determinant one) σ_i-ordinary universal deformation ring. Then $R_{\mathrm{ord}}^{\mathrm{univ}} = \mathbb{Z}_p[[t_1, t_2]]$.*

Proof: By conjugating $\bar{\rho}$ and interchanging σ_0 and σ_1 if necessary, we may assume that $i = 0$, and that $\bar{\rho}(\sigma_0) = \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. Moreover, every σ_0-ordinary deformation ρ of $\bar{\rho}$ has a representative satisfying $\rho(\sigma_0) = \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. Once again, we may apply the same argument as for R^{univ} above to show that $R_{\mathrm{ord}}^{\mathrm{univ}}$ is a power series ring with coefficients in $W(k)$, except that we must lift $\rho^{\mathrm{univ}}(\sigma_0)$ to a matrix of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ and $\rho^{\mathrm{univ}}(\sigma_1)$ to a matrix of determinant one in the proof of Proposition 2.20. Moreover, if $R_{\mathrm{ord}}^{\mathrm{univ}}(\bar{\rho} \otimes \mathbb{F}_{p^2}) = W(\mathbb{F}_{p^2})[[t_1, \ldots, t_d]]$, then $R_{\mathrm{ord}}^{\mathrm{univ}} = \mathbb{Z}_p[[t_1, \ldots, t_d]]$. This again follows from the above argument, except that $H^1(\Pi, \mathrm{ad}(\bar{\rho}))$ must be replaced by $H^1(\Pi, \mathrm{ad}_0^{\sigma_0}(\bar{\rho}))$, where $\mathrm{ad}_0^{\sigma_0}(\bar{\rho})$

denotes the subgroup of $\mathrm{ad}_0(\bar{\rho})$ consisting of those matrices whose kernel contains the subspace of k^2 fixed by $\bar{\rho}(\sigma_0)$.

The last paragraph of the proof of Lemma 2.22 shows that we may assume that σ_1 has distinct eigenvalues (in $\mathbb{F}_{p^2}$) by replacing σ_1 with $\sigma_1\sigma_0$ or $\sigma_0\sigma_1\sigma_0$ if necessary. Thus without loss of generality, any σ_0-ordinary deformation ρ of $\bar{\rho} \otimes \mathbb{F}_{p^2}$ to a ring R has a unique representative of the form $\rho(\sigma_0) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\rho(\sigma_1) = \left(\begin{smallmatrix} \alpha+m_1 & 0 \\ \beta+m_2 & (\alpha+m_1)^{-1} \end{smallmatrix}\right)$ for some $m_1, m_2 \in \mathfrak{m}_R$, where $\alpha, \beta \in W(\mathbb{F}_{p^2})$ are fixed. An argument similar to that in the proof of Theorem 2.27 shows that $R^{\mathrm{univ}}_{\mathrm{ord}}(\bar{\rho} \otimes \mathbb{F}_{p^2}) = W(\mathbb{F}_{p^2})[[t_1, t_2]]$, where the corresponding universal deformation $\rho^{\mathrm{univ}}_{\mathrm{ord}}$ is given by $\rho^{\mathrm{univ}}_{\mathrm{ord}}(\sigma_0) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\rho^{\mathrm{univ}}_{\mathrm{ord}}(\sigma_1) = \left(\begin{smallmatrix} \alpha+t_1 & 0 \\ \beta+t_2 & (\alpha+t_1)^{-1} \end{smallmatrix}\right)$. Therefore, by the above remarks, $R^{\mathrm{univ}}_{\mathrm{ord}} = \mathbb{Z}_p[[t_1, t_2]]$. $\square$

If $\bar{\rho}(\sigma_i) \sim \left(\begin{smallmatrix} -1 & * \\ 0 & -1 \end{smallmatrix}\right)$, then by abuse of language we will also say that a deformation ρ of $\bar{\rho}$ is σ_i-ordinary if $\rho(\sigma_i) \sim \left(\begin{smallmatrix} -1 & * \\ 0 & -1 \end{smallmatrix}\right)$.

Corollary 2.30 *Let σ_0 and σ_1 be as in Theorem* 2.29. *Suppose that for $i = 0$ or* 1, *$\bar{\rho}(\sigma_i) \sim \left(\begin{smallmatrix} -1 & * \\ 0 & -1 \end{smallmatrix}\right)$. Then there is a universal σ_i-ordinary deformation $(R^{\mathrm{univ}}_{\mathrm{ord}}, \rho^{\mathrm{univ}}_{\mathrm{ord}})$, and $R^{\mathrm{univ}}_{\mathrm{ord}} = \mathbb{Z}_p[[t_1, t_2]]$.*

Proof: Without loss of generality, we may assume that $i = 0$. Given any deformation ρ of any residual representation $\bar{\rho}$, let ρ_- denote the deformation given by $\rho_-(\sigma_0) = -\rho(\sigma_0)$ and $\rho_-(\sigma_1) = \rho(\sigma_1)$. Since $\bar{\rho}(\sigma_0) \sim \left(\begin{smallmatrix} -1 & * \\ 0 & -1 \end{smallmatrix}\right)$, we have $\bar{\rho}_-(\sigma_0) \sim \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. Since $\bar{\rho}$ is absolutely irreducible, so is $\bar{\rho}_-$; hence by Theorem 2.29, there is a universal σ_0-ordinary deformation $\rho^{\mathrm{univ}}_{-\mathrm{ord}}$ corresponding to $\bar{\rho}_-$, with $R^{\mathrm{univ}}_{-\mathrm{ord}} = \mathbb{Z}_p[[t_1, t_2]]$. The universal σ_0-ordinary deformation of $\bar{\rho}$ is given by $(\rho^{\mathrm{univ}}_{-\mathrm{ord}})_-$. $\square$

Let $S \subset \Pi$ be a finite set. We say that a deformation ρ of $\bar{\rho} : \Pi \longrightarrow \mathrm{GL}_2(k)$ is *S-ordinary* if ρ is σ-ordinary for every $\sigma \in S$. Assuming that $\bar{\rho}$ is itself

S-ordinary, we once again obtain a universal deformation $(R^{\mathrm{univ}}_{S-\mathrm{ord}}, \rho^{\mathrm{univ}}_{S-\mathrm{ord}})$.

Theorem 2.31 *Let Π be as above, σ_0, σ_1 topological generators of Π. Let $S = \{\sigma_0, \sigma_1\}$, and suppose that $\bar{\rho} : \Pi \longrightarrow \mathrm{SL}_2(\mathbb{F}_p)$ is an S-ordinary residual representation. Then $R^{\mathrm{univ}}_{S-\mathrm{ord}} = \mathbb{Z}_p[[t]]$, and $\rho^{\mathrm{univ}}_{S-\mathrm{ord}}$ is conjugate to the deformation ρ given by*

$$\rho(\sigma_0) = \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \textit{and} \quad \rho(\sigma_1) = \pm \begin{pmatrix} 1 & 0 \\ \alpha + t & 1 \end{pmatrix}$$

for some $\alpha \in \mathbb{Z}_p$, where the sign of each $\rho(\sigma_i)$ corresponds to the sign of the eigenvalue ± 1 of $\bar{\rho}(\sigma_i)$.

Proof: Conjugating $\bar{\rho}$ if necessary and applying a similar argument to that in the proof of Corollary 2.30, we may assume that $\bar{\rho}(\sigma_0) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\bar{\rho}(\sigma_1) = \left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)$. Fix a lift $\alpha \in \mathbb{Z}_p$ of a. Any S-ordinary deformation ρ of $\bar{\rho}$ to R has a unique representative of the form $\rho(\sigma_0) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\rho(\sigma_1) = \left(\begin{smallmatrix} 1 & 0 \\ \alpha + m & 1 \end{smallmatrix}\right)$ for some $m \in \mathfrak{m}_R$. The same argument as for the universal deformations above now gives the result. $\square$

3 Lowering the Field of Definition

3.1 The Cyclotomic Character

Let $\widehat{\overline{\mathbb{Q}}(t)}$ denote the maximal algebraic extension of $\overline{\mathbb{Q}}(t)$ unramified outside three places, each of which is fixed by $\mathrm{Gal}\left(\overline{\mathbb{Q}}(t)/\mathbb{Q}(t)\right)$, and let $\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2$ denote the valuation ideals corresponding to these places. By Theorem 2.7, there exist topological generators $\gamma_0, \gamma_1, \gamma_2$ of inertia groups above $\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2$ respectively, which topologically generate $\Pi := \mathrm{Gal}\left(\widehat{\overline{\mathbb{Q}}(t)}/\overline{\mathbb{Q}}(t)\right)$, and satisfy $\gamma_0\gamma_1\gamma_2 = 1$. By the fundamental theorem of infinite Galois theory, Π is a normal subgroup of $\Gamma_{\mathbb{Q}} := \mathrm{Gal}\left(\widehat{\overline{\mathbb{Q}}(t)}/\mathbb{Q}(t)\right)$; thus $\Gamma_{\mathbb{Q}}$ acts on Π by conjugation.

The action of $\sigma \in \Gamma_{\mathbb{Q}}$ on Π is determined up to conjugation in Π by the restriction $\bar{\sigma}$ of σ to $\overline{\mathbb{Q}}(t)$. Viewing $\bar{\sigma}$ as an element of $G_{\mathbb{Q}}$ via the natural isomorphism $\mathrm{Gal}\left(\overline{\mathbb{Q}}(t)/\mathbb{Q}(t)\right) \cong G_{\mathbb{Q}}$, the action of σ on each γ_i is determined up to conjugation in Π by the action of $\bar{\sigma}$ on the roots of unity in $\overline{\mathbb{Q}}$. To make this explicit, we define the *cyclotomic character* χ as follows: let $\widehat{\mathbb{Z}} := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$, and fix a compatible system $(\zeta_n)_{n\in\mathbb{N}}$ of primitive nth roots of unity ζ_n. Given $\bar{\sigma} \in G_{\mathbb{Q}}$, for each $n \in \mathbb{N}$ we have

$$\bar{\sigma}(\zeta_n) = \zeta_n^{\chi_n(\bar{\sigma})}$$

for some $\chi_n(\bar{\sigma}) \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ which is independent of the choice of ζ_n. Moreover, this action is compatible in the sense that whenever $m|n$, the natural map $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ takes $\chi_n(\bar{\sigma})$ to $\chi_m(\bar{\sigma})$. Thus $(\chi_n(\bar{\sigma}))_{n\in\mathbb{N}} \in \widehat{\mathbb{Z}}^{\times}$, and we define the cyclotomic character $\chi : G_{\mathbb{Q}} \longrightarrow \widehat{\mathbb{Z}}^{\times}$ by $\chi(\bar{\sigma}) = (\chi_n(\bar{\sigma}))_{n\in\mathbb{N}}$. For $\sigma \in \Gamma_{\mathbb{Q}}$, we will often write $\chi(\sigma)$ to mean $\chi(\bar{\sigma})$.

Given any profinite group $G = \varprojlim_{i \in I} G_i$, where each G_i is finite, there is a natural way to define exponentiation in G by elements of $\widehat{\mathbb{Z}}$. Given $(g_i)_{i\in I} \in G$, $\alpha = (\alpha_n)_{n\in\mathbb{N}} \in \widehat{\mathbb{Z}}$, define $(g_i)^\alpha := (g_i^{\alpha_{n(i)}})$ where $n(i) = |G_i|$. The compatibility conditions on (g_i) and on (α_n) ensure that $(g_i^{\alpha_{n(i)}})$ is indeed an element of G.

Theorem 3.1 *For each $\sigma \in \Gamma_{\mathbb{Q}}$ and each $i = 0, 1, 2$,*

$$\gamma_i^\sigma \sim \gamma_i^{\chi(\sigma)},$$

where $\sim$ denotes conjugacy in Π, and χ is the cyclotomic character.

Proof: The proof given here follows that of [MM99], Ch. I, Theorem 2.3. For each $i = 0, 1, 2$, let $\widehat{\mathfrak{p}}_i$ be the valuation ideal of $\widehat{\overline{\mathbb{Q}}(t)}$ such that γ_i generates the inertia group $I_i := I\left(\widehat{\mathfrak{p}}_i/\mathfrak{p}_i\right)$. Since $\sigma(\mathfrak{p}_i) = \mathfrak{p}_i$ for each $i = 0, 1, 2$, we have $I_i^\sigma = I\left(\sigma(\widehat{\mathfrak{p}}_i)/\mathfrak{p}_i\right)$, and in particular $\gamma_i^\sigma \in I\left(\sigma(\widehat{\mathfrak{p}}_i)/\mathfrak{p}_i\right)$. Since Π acts transitively on the primes above $\mathfrak{p}_i$, there is some $\delta \in \Pi$ such that $\delta\left(\sigma(\widehat{\mathfrak{p}}_i)\right) = \widehat{\mathfrak{p}}_i$, and thus $(\gamma_i^\sigma)^\delta \in I_i$. The group I_i is generated by γ_i as a procyclic group, so there is some $\alpha \in \widehat{\mathbb{Z}}$ such that $(\gamma_i^\sigma)^\delta = \gamma_i^\alpha$; in particular, we have $\gamma_i^\sigma \sim \gamma_i^\alpha$.

It remains to show that $\alpha = \chi(\sigma)$. For each $i = 0, 1, 2$, let $f_i \in \mathbb{Q}(t)$ be an element which generates $\mathfrak{p}_i$ in its corresponding valuation ring. For each $i = 0, 1, 2$, $\overline{\mathbb{Q}}(t)(f_i^{1/n})_{n\in\mathbb{N}}$ is an abelian extension of $\overline{\mathbb{Q}}(t)$ contained in $\widehat{\overline{\mathbb{Q}}(t)}$, where we choose each $f_i^{1/n}$ so that they are compatible in the sense that $(f_i^{1/kn})^k = f_i^{1/n}$ for all $k, n \in \mathbb{N}$. We now fix some $i = 0, 1$, or 2. Since

$$\mathbb{Q}(t)(f_i^{1/n})_{n\in\mathbb{N}} \bigcap \overline{\mathbb{Q}}(t) = \mathbb{Q}(t),$$

there is some $\tilde{\sigma} \in \Gamma_{\mathbb{Q}}$ whose restriction to $\overline{\mathbb{Q}}(t)$ is $\bar{\sigma}$, and which fixes $f_i^{1/n}$ for all n. Now $\gamma_i(f_i) = f_i$, so $\gamma_i(f_i^{1/n})$ is an nth root of f_i in $\widehat{\overline{\mathbb{Q}}(t)}$, and is therefore of the form $\zeta_n f_i^{1/n}$ for some nth root of unity ζ_n. Moreover,

$$I\left((f_i^{1/n})/(f_i)\right) = \mathrm{Gal}\left(\overline{\mathbb{Q}}(t)(f_i^{1/n})/\overline{\mathbb{Q}}(t)\right)$$

is generated by the restriction of γ_i to $\overline{\mathbb{Q}}(t)(f_i^{1/n})$, so ζ_n is a primitive nth root of unity, and the various ζ_n obtained in this way are compatible under the canonical maps. Since $\tilde{\sigma}$ restricts to $\bar{\sigma}$, there is some $\delta \in \Pi$ such that $\tilde{\sigma} = \delta\sigma$, and hence $\gamma_i^{\tilde{\sigma}} \sim \gamma_i^{\sigma} \sim \gamma_i^{\alpha}$. Therefore, the restrictions of $\gamma_i^{\tilde{\sigma}}$ and γ_i^{α} to the maximal abelian extension $\widehat{\overline{\mathbb{Q}}(t)}^{\mathrm{ab}}$ of $\overline{\mathbb{Q}}(t)$ in $\widehat{\overline{\mathbb{Q}}(t)}$ are equal; in particular, $\gamma_i^{\alpha}(f_i^{1/n}) = \gamma_i^{\tilde{\sigma}}(f_i^{1/n})$ for all n. Thus we have

$$\begin{aligned}\zeta_n^{\alpha} f_i^{1/n} = \gamma_i^{\alpha}(f_i^{1/n}) = \gamma_i^{\tilde{\sigma}}(f_i^{1/n}) &= \tilde{\sigma}\gamma_i\tilde{\sigma}^{-1}(f_i^{1/n}) \\ &= \tilde{\sigma}\gamma_i(f_i^{1/n}) = \tilde{\sigma}(\zeta_n f_i^{1/n}) = \bar{\sigma}(\zeta_n) f_i^{1/n},\end{aligned}$$

and therefore $\bar{\sigma}(\zeta_n) = \zeta_n^{\alpha}$ for all n, which proves that $\alpha = \chi(\bar{\sigma})$. □

3.2 The Rigidity Theorem

In this section, we introduce the notion of rigidity, which will be used to extend the universal deformation of a given residual representation

$$\bar{\rho} : \Pi \longrightarrow \mathrm{SL}_2(\mathbb{F}_p)$$

to a representation of $\Pi_{K(\boldsymbol{\mu})} := \mathrm{Gal}\left(\widehat{\overline{K}(t)}/K(\boldsymbol{\mu}, t)\right)$, where K is an algebraic extension of $\mathbb{Q}$ and $\boldsymbol{\mu}$ is a collection of roots of unity in $\overline{K}$ which depends on $\bar{\rho}$.

Let G be a group, and let $C_0, \ldots, C_n$ be conjugacy classes in G (not necessarily distinct). We denote by $\bar{\Sigma}(C_0, \ldots, C_n)$ the set of all $n+1$-tuples $(g_0, \ldots, g_n) \in C_0 \times \cdots \times C_n$ which satisfy $g_0 \cdots g_n = 1$. An $n+1$-tuple $(h_0, \ldots, h_n) \in G^{n+1}$ is said to be *locally conjugate* to an element $(g_0, \ldots, g_n)$ of $\bar{\Sigma}(C_0, \ldots, C_n)$ if $(h_0, \ldots, h_n)$ belongs to $\bar{\Sigma}(C_0, \ldots, C_n)$ and the subgroups $\langle g_0, \ldots, g_n \rangle$ and $\langle h_0, \ldots, h_n \rangle$ of G are isomorphic. Note that G acts on $\bar{\Sigma}(C_0, \ldots, C_n)$ by componentwise conjugation; thus for $g \in G$, we will write $(g_0, \ldots, g_n)^g$ to mean $(gg_0g^{-1}, \ldots, gg_ng^{-1})$. Two elements of $\bar{\Sigma}(C_0, \ldots, C_n)$ are said to be *globally conjugate* if they lie in the same G-orbit under this action.

Definition 3.2 *The $n+1$-tuple $(g_0, \ldots, g_n) \in \bar{\Sigma}(C_0, \ldots, C_n)$ is said to be* rigid *if every element of G^{n+1} which is locally conjugate to $(g_0, \ldots, g_n)$ is globally conjugate to $(g_0, \ldots, g_n)$.*

For any algebraic extension K of $\mathbb{Q}$, let $G_K := \mathrm{Gal}(\overline{K}/K)$, and let $\Pi_K := \mathrm{Gal}\left(\widehat{\overline{K}(t)}/K(t)\right)$, where $\widehat{\overline{K}(t)}$ denotes the maximal algebraic extension of $\overline{K}(t)$ unramified outside $0, 1, \infty$. Let $\gamma_0, \gamma_1, \gamma_\infty \in \Pi_{\overline{K}}$ be topological generators of inertia groups I_0, I_1, I_∞ above $0, 1, \infty$ respectively such that $\gamma_0\gamma_1\gamma_\infty = 1$.

Lemma 3.3 (Belyĭ) *For each $i = 0, 1, \infty$, the natural surjection $\Pi_K \twoheadrightarrow G_K$ has a splitting $\phi_i : G_K \hookrightarrow \Pi_K$ whose image is contained in $N_{\Pi_K}(I_i)$.*

Outline of Proof: Without loss of generality, suppose that $i = 0$. Let

$$\Gamma := \left\{\gamma \in \Pi_K : \gamma\gamma_0\gamma^{-1} = \gamma_0^{\chi(\gamma)}, \gamma\gamma_1\gamma^{-1} \approx \gamma_1^{\chi(\gamma)}\right\},$$

where $\approx$ denotes conjugacy by an element of the commutator subgroup $[\Pi_{\overline{K}}, \Pi_{\overline{K}}]$ of $\Pi_{\overline{K}}$, and χ denotes the cyclotomic character. One may show that restricting the natural map $\Pi_K \twoheadrightarrow G_K$ to Γ defines an isomorphism $\Gamma \cong G_K$. Letting ϕ_i be the inverse of this isomorphism gives the result. See [Bel80], §1 for details. $\square$

Corollary 3.4 *The group Π_K is isomorphic to $\Pi_{\overline{K}} \rtimes G_K$.*

The following theorem, which we will use to extend the universal deformations of §2.6, is a variant of the rigidity theorem of Belyĭ, Fried, Matzat, Shih, and Thompson. For other variants, see [Ser92], [Vol96], and [MM99].

Let G be a profinite group, and r the natural map $G \longrightarrow G/Z(G)$. Given any homomorphism $\rho^{\text{geom}} : \Pi_{\overline{K}} \longrightarrow G$, let $\boldsymbol{\mu}$ denote the set of all nth roots of unity in $\overline{K}$ for which $\rho^{\text{geom}}(\gamma_i)$ has exact order n in some finite quotient of G for some $i = 0, 1, \infty$.

Theorem 3.5 *Suppose that $(\rho^{\text{geom}}(\gamma_0), \rho^{\text{geom}}(\gamma_1), \rho^{\text{geom}}(\gamma_\infty))$ forms a rigid triple in G. Suppose moreover that $Z_G(\mathrm{Im}(\rho^{\text{geom}})) = Z(G)$.*
(1) *The composed map $\hat{\rho}^{\text{geom}} := r \circ \rho^{\text{geom}} : \Pi_{\overline{K}} \longrightarrow G/Z(G)$ extends uniquely to a homomorphism $\hat{\rho} : \Pi_{K(\boldsymbol{\mu})} \longrightarrow G/Z(G)$.*
(2) *Let ϕ_i be as in Lemma 3.3, and suppose that for some i the inclusion $Z(G) \hookrightarrow r^{-1}\left(\hat{\rho} \circ \phi_i(G_{K(\boldsymbol{\mu})})\right)$ splits. Then ρ^{geom} extends to a homomorphism $\rho : \Pi_{K(\boldsymbol{\mu})} \longrightarrow G$ which is unique up to multiplication by a homomorphism $\psi : G_K \longrightarrow Z(G)$.*

Proof: Let $\gamma \in \Pi_{K(\boldsymbol{\mu})}$. By Theorem 3.1, $\gamma\gamma_i\gamma^{-1} \sim \gamma_i^{\chi(\gamma)}$ in $\Pi_{\overline{K}}$ for each $i = 0, 1, \infty$, and hence $\rho^{\text{geom}}(\gamma\gamma_i\gamma^{-1}) \sim \rho^{\text{geom}}(\gamma_i)^{\chi(\gamma)}$ in G. Let H be any finite quotient of G, and let n be the order of the image of $\rho^{\text{geom}}(\gamma_i)$ in H. Since

γ fixes $K(\boldsymbol{\mu})$ pointwise and $K(\boldsymbol{\mu})$ contains all of the nth roots of unity in $\overline{K}$, we have $\chi(\gamma) \equiv 1 \mod n$. Therefore $\rho^{\text{geom}}(\gamma_i)^{\chi(\gamma)} = \rho^{\text{geom}}(\gamma_i)$, and hence $\rho^{\text{geom}}(\gamma_i) \sim \rho^{\text{geom}}(\gamma\gamma_i\gamma^{-1})$ in G. For each $i = 0, 1, \infty$, let $\delta_i = \rho^{\text{geom}}(\gamma_i)$, and $\delta_i^\gamma = \rho^{\text{geom}}(\gamma\gamma_i\gamma^{-1})$. Since $\langle \delta_0, \delta_1, \delta_\infty \rangle = \langle \delta_0^\gamma, \delta_1^\gamma, \delta_\infty^\gamma \rangle = \text{Im}\rho^{\text{geom}}$, $(\delta_0^\gamma, \delta_1^\gamma, \delta_\infty^\gamma)$ is locally conjugate to $(\delta_0, \delta_1, \delta_\infty)$ in G; thus by the rigidity of $(\delta_0, \delta_1, \delta_\infty)$, there is some $g_\gamma \in G$ such that $g_\gamma \delta_i g_\gamma^{-1} = \delta_i^\gamma$ for each $i = 0, 1, \infty$. Define a set-theoretic map $\hat{\rho} : \Pi_{K(\boldsymbol{\mu})} \longrightarrow G/Z(G)$ by

$$\hat{\rho}(\gamma) = r(g_\gamma) \in G/Z(G)$$

for all $\gamma \in \Pi_{K(\boldsymbol{\mu})}$. We claim that $\hat{\rho}$ is a homomorphism extending $\hat{\rho}^{\text{geom}}$. Note that $r(g_\gamma)$ is uniquely determined since $Z_G(\text{Im}\rho^{\text{geom}}) = Z(G)$; thus to show that $\hat{\rho}$ is a homomorphism, it suffices to show that given $\gamma, \gamma' \in \Pi_{K(\boldsymbol{\mu})}$, we have

$$g_\gamma g_{\gamma'} \delta_i g_{\gamma'}^{-1} g_\gamma^{-1} = \rho^{\text{geom}}(\gamma\gamma'\gamma_i\gamma'^{-1}\gamma^{-1})$$

for each $i = 0, 1, \infty$. In fact, since $\gamma_0, \gamma_1, \gamma_\infty$ generate $\Pi_{\overline{K}}$, we have $\rho^{\text{geom}}(\gamma\sigma\gamma^{-1}) = g_\gamma \rho^{\text{geom}}(\sigma) g_\gamma^{-1}$ for all $\sigma \in \Pi_{\overline{K}}$, so $\hat{\rho}$ is indeed a homomorphism. The uniqueness of $\hat{\rho}$ follows from the uniqueness of $r(g_\gamma)$ and the fact that for any homomorphism $\hat{\rho} : \Pi_{K(\boldsymbol{\mu})} \longrightarrow G/Z(G)$ extending $\hat{\rho}^{\text{geom}}$, $\hat{\rho}(\gamma\gamma_i\gamma^{-1}) = \hat{\rho}(\gamma)\hat{\rho}^{\text{geom}}(\gamma_i)\hat{\rho}(\gamma)^{-1}$ for each $i = 0, 1, \infty$.

To prove (2), choose i so that the inclusion $Z(G) \hookrightarrow r^{-1}\left(\hat{\rho} \circ \phi_i(G_{K(\boldsymbol{\mu})})\right)$ splits. Let $N = r^{-1}\left(\hat{\rho} \circ \phi_i(G_{K(\boldsymbol{\mu})})\right) \subset G$. Since the inclusion $Z(G) \hookrightarrow N$ splits, the surjection $r|_N : N \longrightarrow N/Z(G)$ is split by some homomorphism

$\psi : N/Z(G) \longrightarrow N$. Thus we obtain a homomorphism

$$\psi \circ \hat{\rho} \circ \phi_i : G_{K(\boldsymbol{\mu})} \longrightarrow G.$$

By Corollary 3.4, $\Pi_{K(\boldsymbol{\mu})} \cong \Pi_{\overline{K}} \rtimes G_{K(\boldsymbol{\mu})}$, so writing $\gamma \in \Pi_{K(\boldsymbol{\mu})}$ as $\gamma = \alpha\beta$ where $\alpha \in \Pi_{\overline{K}}$ and $\beta \in \phi_i(G_{K(\boldsymbol{\mu})})$, we may define a homomorphism $\rho : \Pi_{K(\boldsymbol{\mu})} \longrightarrow G$ extending ρ^{geom} by $\rho(\gamma) = \rho^{\mathrm{geom}}(\alpha)\psi\circ\hat{\rho}(\beta)$. The uniqueness statement follows immediately from that of (1). $\square$

3.3 Rigidity in $\mathrm{GL}_2(R^{\mathrm{univ}})$

The universal deformation rings of Theorems 2.28, 2.29, and 2.31 are power series rings over $\mathbb{Z}_p$; in particular, they are local unique factorization domains (UFDs). Thus in order to extend the corresponding universal deformations using Theorem 3.5, it is necessary to study rigidity in $\mathrm{GL}_2(R)$, where $(R, \mathfrak{m})$ is a local UFD with residue field k. We will show that if ρ is a determinant one deformation of a residual representation $\bar{\rho} : \Pi \longrightarrow \mathrm{GL}_2(k)$ to such a ring R, then $(\rho(\gamma_0), \rho(\gamma_1), \rho(\gamma_\infty))$ is rigid in $\mathrm{GL}_2(R)$.

Definition 3.6 *For any domain R, a subgroup G of $\mathrm{GL}_n(R)$ is said to be* irreducible *if there is no eigenvector common to all elements of G in any domain containing R. The subgroup G is said to be* acentral *in $\mathrm{GL}_n(R)$ if the centralizer $Z_{\mathrm{M}_n(R)}(G)$ of G in the matrix ring $\mathrm{M}_n(R)$ consists only of the scalar matrices.*

If $R = k$ is a field, then G is irreducible if and only if the identity map of G is an absolutely irreducible representation; moreover, by Schur's lemma, every irreducible subgroup is acentral (see [Isa94], p.145).

Proposition 3.7 *Let $(R, \mathfrak{m})$ be a local domain with residue field k, and suppose that $M_0, M_1 \in \mathrm{GL}_2(R)$ have the property that the reductions $\bar{M}_0, \bar{M}_1$ of $M_0, M_1 \mod \mathfrak{m}$ generate an irreducible subgroup of $\mathrm{GL}_2(k)$. Then for any domain $R' \supset R$, the subgroup of $\mathrm{GL}_2(R')$ generated by M_0 and M_1 is both irreducible and acentral.*

Proof: Let λ_0, λ_1 be eigenvalues of M_0, M_1 respectively in some domain containing R. Since λ_0 and λ_1 are integral over R, there is a maximal ideal $\mathfrak{p}$ of $R[\lambda_0, \lambda_1]$ lying above $\mathfrak{m}$ (see [Lan93], Ch. VII, Propositions 1.10, 1.11). Let $\mathbf{v}_0, \mathbf{v}_1 \in R[\lambda_0, \lambda_1]^2_{\mathfrak{p}}$ be eigenvectors corresponding to λ_0, λ_1 respectively. The reductions of $\mathbf{v}_0$ and $\mathbf{v}_1 \mod \mathfrak{p}$ must be distinct, for otherwise $R[\lambda_0, \lambda_1]_{\mathfrak{p}}/\mathfrak{p}$ is an extension of k in which $\bar{M}_0, \bar{M}_1$ have a common eigenvector; in particular, $\mathbf{v}_0$ and $\mathbf{v}_1$ are distinct. Therefore M_0 and M_1 generate an irreducible subgroup G of $\mathrm{GL}_2(R)$, and hence also of $\mathrm{GL}_2(R')$ where R' is any domain containing R. Furthermore, G is an irreducible and thus acentral subgroup of $\mathrm{GL}_2(\mathrm{Qu}(R'))$. Since

$$Z_{\mathrm{GL}_2(R')}(G) = Z_{\mathrm{GL}_2(\mathrm{Qu}(R'))}(G) \bigcap \mathrm{GL}_2(R'),$$

G is also an acentral subgroup of $\mathrm{GL}_2(R')$. $\square$

In proving the rigidity of certain triples (M_0, M_1, M_2) of matrices in $\mathrm{GL}_2(R)$, the easiest case occurs when M_0 and M_1 both have eigenvalues in R. The following lemmas will allow us to extend R to a domain in which M_0 and M_1 have eigenvalues, then descend to obtain conjugacy in $\mathrm{GL}_2(R)$.

Lemma 3.8 *Let L be a quadratic extension of a field K. Suppose that the pair $M_0, M_1 \in \mathrm{GL}_2(K)$ generates an irreducible subgroup of $\mathrm{GL}_2(K)$, and* *that* $(M_0', M_1') \in \mathrm{GL}_2(K)^2$ *is conjugate to* (M_0, M_1) *by an element of* $\mathrm{GL}_2(L)$. *Then* (M_0', M_1') *is conjugate to* (M_0, M_1) *by an element of* $\mathrm{GL}_2(K)$.

Proof: Let σ denote the nontrivial element of $\mathrm{Gal}(L/K)$, and G the subgroup of $\mathrm{GL}_2(K)$ generated by M_0 and M_1. Let $M \in \mathrm{GL}_2(L)$ be such that $MM_iM^{-1} = M_i'$ for $i = 0, 1$. Since $M_i, M_i' \in \mathrm{GL}_2(K)$, applying σ gives

$$\sigma(M)M_i\sigma(M)^{-1} = M_i' = MM_iM^{-1},$$

and therefore $M^{-1}\sigma(M) \in Z_{\mathrm{M}_2(L)}(G)$. By Proposition 3.7, since G is an irreducible subgroup of $\mathrm{GL}_2(K)$, it is an acentral subgroup of $\mathrm{GL}_2(L)$. Thus $M^{-1}\sigma(M) = \zeta\mathrm{Id}$ for some $\zeta \in L$. Applying σ to the equation $\sigma(M) = \zeta M$ gives $M = \sigma(\zeta)\sigma(M) = \sigma(\zeta)\zeta M$, and therefore $\sigma(\zeta)\zeta = 1$. By Hilbert's Theorem 90, there exists some $\alpha \in L^\times$ such that $\zeta = \frac{\alpha}{\sigma(\alpha)}$. Hence we have $\sigma(\alpha)\sigma(M) = \alpha M$, so αM is invariant under $\mathrm{Gal}(L/K)$, and therefore $\alpha M \in \mathrm{GL}_2(K)$. Conjugating each M_i by αM gives $(\alpha M)M_i(\alpha M)^{-1} = M_i'$, as desired. □

Lemma 3.9 *Let* $(R, \mathfrak{m})$ *be a local UFD with residue field* k *and quotient field* K. *Suppose that the reductions* $\bmod\ \mathfrak{m}$ *of* $M_0, M_1 \in \mathrm{GL}_2(R)$ *together generate an irreducible subgroup of* $\mathrm{GL}_2(k)$, *and that* $(M_0', M_1') \in \mathrm{GL}_2(R)^2$ *is conjugate to* (M_0, M_1) *by an element of* $\mathrm{GL}_2(K)$. *Then* (M_0', M_1') *is conjugate to* (M_0, M_1) *by an element of* $\mathrm{GL}_2(R)$.

Proof: Let $M \in \mathrm{GL}_2(K)$ be such that $MM_iM^{-1} = M_i'$ for $i = 0, 1$. Multiplying M by a suitable scalar, we may assume that $M \in \mathrm{M}_2(R)$, $\det(M) \neq 0$, and $\det(M)$ has minimal $\mathfrak{m}$-adic valuation among all such multiples of M.

Let $M^* = \det(M)M^{-1} \in \mathrm{M}_2(R)$. If $\det(M) \in R^\times$ then we are done. Otherwise, there is an irreducible element $\alpha \in R$ which divides $\det(M)$. We will show that α divides each entry of M, and therefore $\frac{1}{\alpha}M \in \mathrm{M}_2(R)$ is such that $\det(\frac{1}{\alpha}M)$ has lesser $\mathfrak{m}$-adic valuation than $\det(M)$, contradicting the assumption on M.

Since R is a UFD and α is irreducible, $\mathfrak{p} = (\alpha)$ is a prime ideal. Let G be the subgroup of $\mathrm{GL}_2(R)$ generated by M_0 and M_1, let $\tilde{k} = R_\mathfrak{p}/\mathfrak{p}$, and let $\tilde{G}$ denote the subgroup of $\mathrm{GL}_2(\tilde{k})$ obtained by taking the mod $\mathfrak{p}$ reduction of G viewed as a subgroup of $\mathrm{GL}_2(R_\mathfrak{p})$. The diagram

$$\begin{tikzcd}
R \arrow[r, hook] \arrow[d] & R_\mathfrak{p} \arrow[d] \\
R/\mathfrak{p} \arrow[r, hook, "\mathrm{Qu}"'] \arrow[d] & \tilde{k} \\
k &
\end{tikzcd}$$

commutes, where the injection $R/\mathfrak{p} \hookrightarrow \tilde{k}$ is obtained by viewing $\tilde{k}$ as the quotient field of $R/\mathfrak{p}$. Since k is the residue field of $R/\mathfrak{p}$ and the reduction $\bar{G}$ of $G \mod \mathfrak{m}$ is an irreducible subgroup of $\mathrm{GL}_2(k)$, by Proposition 3.7, the reduction of $G \mod \mathfrak{p}$ is an irreducible subgroup of $\mathrm{GL}_2(R/\mathfrak{p})$; hence $\tilde{G}$ is an irreducible subgroup of $\mathrm{GL}_2(\tilde{k})$. Therefore, $\tilde{G}$ generates the $\tilde{k}$-algebra $\mathrm{M}_2(\tilde{k})$ (see [Isa94], p.145).

For any $A \in \mathrm{M}_2(R)$, let $\tilde{A} \in \mathrm{M}_2(\tilde{k})$ denote the element obtained by viewing A as an element of $\mathrm{M}_2(R_\mathfrak{p})$ and reducing mod $\mathfrak{p}$. Each $\tilde{A} \in \mathrm{M}_2(\tilde{k})$ may be expressed as a $\tilde{k}$-linear combination of elements of $\tilde{G}$, say

$$\tilde{A} = \tilde{\alpha}_0\tilde{A}_0 + \cdots + \tilde{\alpha}_r\tilde{A}_r.$$

For each $i = 0, \ldots, r$, choose $A_i \in G$ reducing to $\tilde{A}_i \mod \mathfrak{p}$, and $\alpha_i \in R_\mathfrak{p}$ reducing to $\tilde{\alpha}_i \mod \mathfrak{p}$. Since $A_i \in G = \langle M_0, M_1 \rangle$ for each $i = 0, \ldots, r$, the lift $A = \alpha_0 A_0 + \cdots + \alpha_r A_r \in \mathrm{M}_2(R_\mathfrak{p})$ of $\tilde{A}$ satisfies $MAM^{-1} \in \mathrm{M}_2(R_\mathfrak{p})$. Hence $MAM^* \in \det(M)\mathrm{M}_2(R_\mathfrak{p})$, and reducing mod $\mathfrak{p}$ gives $\tilde{M}\tilde{A}\tilde{M}^* = 0$. Let $\tilde{M} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Taking $\tilde{A} = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ gives $0 = \tilde{M}\tilde{A}\tilde{M}^* = \begin{pmatrix} -ac & a^2 \\ -c^2 & ac \end{pmatrix}$ and hence $a = c = 0$. Taking $\tilde{A} = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ similarly gives $b = d = 0$ and therefore $\tilde{M} = 0$; that is, $M \in \mathrm{M}_2(\mathfrak{p})$, so α divides each entry of M, which gives the desired contradiction. $\square$

We now prove the main result of this section:

Theorem 3.10 *Let R be a local UFD with residue field k, and suppose that (M_0, M_1, M_2) is a triple of matrices in $\mathrm{SL}_2(R)$ satisfying $M_0M_1M_2 = 1$, whose reductions* mod $\mathfrak{m}$ *together generate an irreducible subgroup of* $\mathrm{GL}_2(k)$. *Then (M_0, M_1, M_2) is rigid in* $\mathrm{GL}_2(R)$.

Proof: Let $K = \mathrm{Qu}(R)$, and $L = K(\lambda_0, \lambda_1)$, where λ_0, λ_1 are eigenvalues of M_0, M_1 respectively. Choosing a basis for L^2, we view M_0 and M_1 as linear transformations of L^2 with respect to this basis. By Proposition 3.7, M_0 and M_1 generate an irreducible subgroup of $\mathrm{GL}_2(R)$, and also of $\mathrm{GL}_2(L)$; hence choosing eigenvectors $\mathbf{v}_0, \mathbf{v}_1 \in L^2$ corresponding to the eigenvalues λ_0, λ_1 gives a basis $\{\mathbf{v}_0, \mathbf{v}_1\}$ for L^2. Writing (M_0, M_1, M_2) with respect to this basis gives a triple $(\tilde{M}_0, \tilde{M}_1, \tilde{M}_2)$ globally conjugate to (M_0, M_1, M_2) in $\mathrm{GL}_2(L)$ such that $\tilde{M}_0 = \left(\begin{smallmatrix} \alpha & \gamma \\ 0 & \alpha^{-1} \end{smallmatrix}\right)$ and $\tilde{M}_1 = \begin{pmatrix} \beta & 0 \\ \delta & \beta^{-1} \end{pmatrix}$ for some $\alpha, \beta, \delta, \gamma \in L^\times$. Rescaling $\{\mathbf{v}_0, \mathbf{v}_1\}$ if necessary, we may assume that $\gamma = 1$.

Let (M_0', M_1', M_2') be any triple of matrices which is locally conjugate to (M_0, M_1, M_2) in $\mathrm{GL}_2(R)$, and which satisfies $M_0'M_1'M_2' = 1$. Since $M_0 \sim M_0'$ and $M_1 \sim M_1'$, $\lambda_0, \lambda_1 \in L$ are eigenvalues of M_0', M_1' respectively. Thus by the same reasoning as for (M_0, M_1, M_2) above, there is a triple $(\tilde{M}'_0, \tilde{M}'_1, \tilde{M}'_2)$ globally conjugate to (M'_0, M'_1, M'_2) in $\mathrm{GL}_2(L)$ such that $\tilde{M}'_0 = \left(\begin{smallmatrix} \alpha' & 1 \\ 0 & \alpha'^{-1} \end{smallmatrix}\right)$ and $\tilde{M}'_1 = \left(\begin{smallmatrix} \beta' & 0 \\ \delta' & \beta'^{-1} \end{smallmatrix}\right)$ for some $\alpha', \beta', \delta' \in L^\times$. Now $\tilde{M}_0 \sim \tilde{M}'_0$ implies that $\mathrm{Tr}(\tilde{M}_0) = \mathrm{Tr}(\tilde{M}'_0)$; that is, $\alpha + \alpha^{-1} = \alpha' + \alpha'^{-1}$. Hence $(\alpha - \alpha')(\alpha\alpha' - 1) = 0$, and therefore $\alpha = \alpha'$ or $\alpha = \alpha'^{-1}$. If $\alpha = \alpha'^{-1} \neq \alpha'$, then conjugating $(\tilde{M}_0, \tilde{M}_1, \tilde{M}_2)$ by $M = \left(\begin{smallmatrix} 1 & 0 \\ \alpha' - \alpha'^{-1} & 1 \end{smallmatrix}\right)$ gives $M\tilde{M}_0M^{-1} = \left(\begin{smallmatrix} \alpha'^{-1} & 1 \\ 0 & \alpha' \end{smallmatrix}\right)$ and $M\tilde{M}'_1M^{-1} = \left(\begin{smallmatrix} \beta' & 0 \\ * & \beta'^{-1} \end{smallmatrix}\right)$. Thus replacing $(\tilde{M}'_0, \tilde{M}'_1, \tilde{M}'_2)$ with $(\tilde{M}'_0, \tilde{M}'_1, \tilde{M}'_2)^M$ if necessary, and renaming α', δ' accordingly, we have $\alpha = \alpha'$. Similarly, $\mathrm{Tr}(\tilde{M}_1) = \mathrm{Tr}(\tilde{M}'_1)$ gives $\beta = \beta'$ or $\beta = \beta'^{-1}$. If $\beta = \beta'^{-1} \neq \beta'$, then taking $M = \left(\begin{smallmatrix} \delta' & \beta'^{-1} - \beta' \\ 0 & \delta' \end{smallmatrix}\right)$ gives $M\tilde{M}'_0M^{-1} = \tilde{M}'_0$ and $M\tilde{M}'_1M^{-1} = \left(\begin{smallmatrix} \beta'^{-1} & 0 \\ \delta' & \beta' \end{smallmatrix}\right)$, so replacing $(\tilde{M}'_0, \tilde{M}'_1, \tilde{M}'_2)$ with $(\tilde{M}'_0, \tilde{M}'_1, \tilde{M}'_2)^M$ if necessary gives $\beta = \beta'$, and does not affect $\tilde{M}'_0$. Multiplying gives

$$\tilde{M}_2 = (\tilde{M}_0\tilde{M}_1)^{-1} = \begin{pmatrix} \alpha^{-1}\beta^{-1} & -\beta^{-1} \\ -\alpha^{-1}\delta & \alpha\beta + \delta \end{pmatrix},$$

and similarly for $\tilde{M}'_2$; thus the equation $\mathrm{Tr}(\tilde{M}_2) = \mathrm{Tr}(\tilde{M}'_2)$ becomes

$$\alpha^{-1}\beta^{-1} + \alpha\beta + \delta = \alpha'^{-1}\beta'^{-1} + \alpha'\beta' + \delta',$$

and therefore $\delta = \delta'$. Thus we have shown that $(\tilde{M}_0, \tilde{M}_1, \tilde{M}_2) = (\tilde{M}'_0, \tilde{M}'_1, \tilde{M}'_2)$; in particular, (M_0, M_1, M_2) is globally conjugate to (M'_0, M'_1, M'_2) in $\mathrm{GL}_2(L)$.

In order to obtain global conjugacy in $\mathrm{GL}_2(R)$, first note that either $L = K(\lambda_0)$ or L is a quadratic extension of $K(\lambda_0)$. In the latter case, by Proposition 3.7, M_0, M_1 generate an irreducible subgroup of $\mathrm{GL}_2(K(\lambda_0))$; hence by Lemma 3.8, (M_0, M_1, M_2) is globally conjugate to (M'_0, M'_1, M'_2) in

$\mathrm{GL}_2(K(\lambda_0))$. Applying Lemma 3.8 again if necessary (that is, if $K(\lambda_0) \neq K$), we find that (M_0, M_1, M_2) is globally conjugate to (M_0', M_1', M_2') in $\mathrm{GL}_2(K)$. Since R is a UFD, by Lemma 3.9, (M_0, M_1, M_2) is globally conjugate to $(M_0' M_1', M_2')$ in $\mathrm{GL}_2(R)$. Therefore, (M_0, M_1, M_2) is rigid. $\square$

A similar argument to that in the proof of Theorem 3.10 can be used to prove the result for any local domain R, provided that M_0 and M_1 both have eigenvalues in R. In this case, it is not necessary to pass to the field L; the arguments used above can be applied in R itself. In fact, this argument can be extended to prove the result for any local domain R provided that at least one of M_0 and M_1 has an eigenvalue in R, although the details are significantly more complicated. New difficulties arise when neither M_0 nor M_1 has an eigenvalue in R, and it is not clear whether the assumption of unique factorization is necessary in this case.

3.4 Extending the Universal Deformation

We will now use the rigidity theorem of §3.2 to extend the universal deformations of §2.6 to representations of a larger Galois group. Let K be any algebraic extension of $\mathbb{Q}$, and let $\Pi_K, \gamma_0, \gamma_1, \gamma_\infty$ be as in §3.2. Let

$$\rho^{\mathrm{geom}} : \Pi_{\overline{K}} \longrightarrow \mathrm{SL}_2(R)$$

be any representative of one of the following universal deformations:

(1) the $\{\gamma_0, \gamma_1\}$-ordinary universal deformation of Theorem 2.31, in which case $R = \mathbb{Z}_p[[t]]$;

(2) the γ_i-ordinary universal deformation of either Theorem 2.29 or Corol-

lary 2.30, in which case $R = \mathbb{Z}_p[[t_1, t_2]]$; or

(3) the (determinant one) universal deformation of Theorem 2.28, in which case $R = \mathbb{Z}_p[[t_1, t_2, t_3]]$.

Theorem 3.11 *The projectivization*

$$\hat{\rho}^{\text{geom}} : \Pi_{\overline{K}} \longrightarrow \mathrm{PGL}_2(R) = \mathrm{GL}_2(R)/R^\times$$

of ρ can be extended uniquely to a representation $\hat{\rho} : \Pi_{K(\boldsymbol{\mu})} \longrightarrow \mathrm{PGL}_2(R)$, where $\boldsymbol{\mu}$ is as in Theorem 3.5

Proof: Since $\bar{\rho}(\gamma_0), \bar{\rho}(\gamma_1), \bar{\rho}(\gamma_\infty)$ generate an irreducible subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ and R is a local UFD, by Theorem 3.10, $(\rho^{\text{geom}}(\gamma_0), \rho^{\text{geom}}(\gamma_1), \rho^{\text{geom}}(\gamma_\infty))$ is rigid in $\mathrm{GL}_2(R)$. By Proposition 3.7, $\rho^{\text{geom}}(\gamma_0)$ and $\rho^{\text{geom}}(\gamma_1)$ generate an acentral subgroup of $\mathrm{GL}_2(R)$, so $Z_{\mathrm{GL}_2(R)}(\mathrm{Im}\rho^{\text{geom}}) = R^\times = Z(\mathrm{GL}_2(R))$. The result now follows from Theorem 3.5(1). $\square$

Remark. Given a residual representation $\bar{\rho} : \Pi_{\overline{K}} \longrightarrow \mathrm{SL}_2(\mathbb{F}_p)$, let m denote the prime-to-p part of $\operatorname*{lcm}_{i=0,1,\infty}(o(\bar{\rho}(\gamma_i)))$, where $o(\bar{\rho}(\gamma_i))$ denotes the order of $\bar{\rho}(\gamma_i)$ (in particular, $m \mid p^2 - 1$). Let μ_m denote the set of mth roots of unity and μ_{p^∞} the set of all p^nth roots of unity in $\overline{K}$. Note that the kernel of the reduction map $\mathrm{GL}_2(R) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$ is equal to $1 + \mathrm{M}_2(\mathfrak{m}) \cong \mathrm{M}_2(\mathfrak{m})$, and $\mathrm{M}_2(\mathfrak{m}) = \varprojlim \mathrm{M}_2(\mathfrak{m}/\mathfrak{m}^n)$ is an inverse limit of p-groups, so the image of $\rho^{\text{geom}}(\gamma_i)$ in any finite quotient of $\mathrm{GL}_2(R)$ has order dividing $p^n m$ for some n. Therefore, $K(\boldsymbol{\mu})$ is contained in $K(\mu_m, \mu_{p^\infty})$.

Let $\bar{\rho}$ denote the residual representation of ρ^{geom}. If $\bar{\rho}(\gamma_i)$ has an eigenvalue in $\mathbb{F}_p$ for some $i = 0, 1, \infty$, then the above result can be strengthened.

Theorem 3.12 *If ρ^{geom} is the universal deformation of case* (3)*, suppose that $\bar{\rho}(\gamma_i)$ has distinct eigenvalues in $\mathbb{F}_p$ for some $i = 0, 1, \infty$. Then in all three cases, ρ^{geom} extends to a representation $\rho : \Pi_{K(\boldsymbol{\mu})} \longrightarrow \mathrm{GL}_2(R)$ which is unique up to multiplication by a representation $\psi : G_{K(\boldsymbol{\mu})} \longrightarrow R^\times$.*

Proof: Let $\hat{\rho}$ be as in Theorem 3.11. With the notation of §3.2, if we show that for some i the inclusion

$$Z(\mathrm{GL}_2(R)) \hookrightarrow r^{-1}(\hat{\rho} \circ \phi_i(G_{K(\boldsymbol{\mu})}))$$

splits, then the result will follow from Theorem 3.5(2). In all three cases, $\rho^{\text{geom}}(\gamma_i)$ has a rank one eigenspace $V \subset R^2$ for some $i = 0, 1, \infty$ (in case (3), this follows from the argument of Lemma 2.25). Fix such an i, and let $N = r^{-1}(\hat{\rho} \circ \phi_i(G_{K(\boldsymbol{\mu})}))$. We claim that N fixes V. From the proof of Lemma 3.3, for each $\gamma \in \phi_i(G_{K(\boldsymbol{\mu})})$, we have $\gamma\gamma_i\gamma^{-1} = \gamma_i^{\chi(\gamma)}$; applying ρ^{geom} gives $\rho^{\text{geom}}(\gamma\gamma_i\gamma^{-1}) = \rho^{\text{geom}}(\gamma_i)^{\chi(\gamma)}$. Since $K(\boldsymbol{\mu}) \supset K(\mu_m, \mu_{p^\infty})$, and $\rho^{\text{geom}}(\gamma_i)$ has order dividing $p^n m$ (for some n) in every finite quotient of $\mathrm{GL}_2(R)$, we have $\rho^{\text{geom}}(\gamma_i)^{\chi(\gamma)} = \rho^{\text{geom}}(\gamma_i)$, so $\rho^{\text{geom}}(\gamma\gamma_i\gamma^{-1}) = \rho^{\text{geom}}(\gamma_i)$. From the definition of $\hat{\rho}$ in the proof of Theorem 3.5 and the fact that $\ker(r) = Z(\mathrm{GL}_2(R))$, it follows that $\rho^{\text{geom}}(\gamma\gamma_i\gamma^{-1}) = g_\gamma\rho^{\text{geom}}(\gamma_i)g_\gamma^{-1}$ for any $g_\gamma \in r^{-1}(\hat{\rho}(\gamma))$. Every $M \in N$ can be obtained as g_γ for some γ, so $M\rho^{\text{geom}}(\gamma_i)M^{-1} = \rho^{\text{geom}}(\gamma_i)$ for all $M \in N$.

Let λ be the eigenvalue of $\rho^{\text{geom}}(\gamma_i)$ corresponding to $V = R\mathbf{v}$. Since $M\rho^{\text{geom}}(\gamma_i)M^{-1}\mathbf{v} = \lambda\mathbf{v}$, we have

$$\rho^{\text{geom}}(\gamma_i)(M^{-1}\mathbf{v}) = \lambda M^{-1}\mathbf{v},$$

so $M^{-1}\mathbf{v}$ is an eigenvector of $\rho^{\text{geom}}(\gamma_i)$ with eigenvalue λ. Since V is the full eigenspace of $\rho^{\text{geom}}(\gamma_i)$ with eigenvalue λ, we must have $M^{-1}\mathbf{v} \in V$. Therefore, N fixes V, as claimed. Thus each $M \in N$ induces a linear map on R^2/V, which is a free R-module of rank one. Fixing an isomorphism

$$\mathrm{GL}(R^2/V) \cong R^\times = Z(\mathrm{GL}_2(R))$$

gives the desired splitting. $\square$

If the residual representation $\bar{\rho}$ is γ_i-ordinary, the universal property of the determinant one universal deformation ρ^{univ} gives a map $R^{\text{univ}} \longrightarrow R^{\text{univ}}_{\text{ord}}$ which takes any extension of ρ^{univ} to an extension of $\rho^{\text{univ}}_{\text{ord}}$. Similarly, if $\bar{\rho}$ is S-ordinary, where $S = \{\gamma_0, \gamma_1\}$, we obtain maps $R^{\text{univ}} \longrightarrow R^{\text{univ}}_{S-\text{ord}}$ and $R^{\text{univ}}_{\gamma_i-\text{ord}} \longrightarrow R^{\text{univ}}_{S-\text{ord}}$ for each $i = 0, 1$, which take extensions of ρ^{univ} and $\rho^{\text{univ}}_{\gamma_i-\text{ord}}$ respectively to extensions of $\rho^{\text{univ}}_{S-\text{ord}}$. Furthermore, the map $R^{\text{univ}} \longrightarrow R^{\text{univ}}_{S-\text{ord}}$ factors through both maps $R^{\text{univ}}_{\gamma_i-\text{ord}} \longrightarrow R^{\text{univ}}_{S-\text{ord}}$ via the map $R^{\text{univ}} \longrightarrow R^{\text{univ}}_{\gamma_i-\text{ord}}$ discussed above.

4 Geometric Construction of Universal Deformations

4.1 Jacobians of Curves

Fix an odd prime p. Let $\bar{\rho} : \Pi_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$ be the representation describing the action of $\Pi_{\mathbb{Q}}$ on the p-torsion points of the Legendre family E_L of elliptic curves over $\mathbb{Q}(t)$, given by the equation

$$E_L : y^2 = x(x-1)(x-t).$$

Let $\bar{\rho}^{\mathrm{geom}} : \Pi \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$ denote the restriction of $\bar{\rho}$ to $\Pi = \Pi_{\overline{\mathbb{Q}}}$, and let $\sigma_0, \sigma_1, \sigma_\infty \in \Pi$ be generators of inertia groups at $0, 1, \infty$ respectively such that $\sigma_0\sigma_1\sigma_\infty = 1$. Then $\bar{\rho}^{\mathrm{geom}}$ is an absolutely irreducible representation characterized up to conjugation by the property that $\bar{\rho}^{\mathrm{geom}}(\sigma_0)$ and $\bar{\rho}^{\mathrm{geom}}(\sigma_1)$ both have order p and $\bar{\rho}^{\mathrm{geom}}(\sigma_\infty)$ has order $2p$ (see [Dar00], p.419). Let $S = \{\sigma_0, \sigma_1\}$. In this chapter, we give an explicit geometric construction of the S-ordinary universal deformation $\rho^{\mathrm{univ}}_{S-\mathrm{ord}}$ of $\bar{\rho}^{\mathrm{geom}}$. In fact, the representation that we construct will be a representation of the larger Galois group $\Pi_{\mathbb{Q}(\mu_{p^\infty})}$, and thus will be the extension of $\rho^{\mathrm{univ}}_{S-\mathrm{ord}}$ given in Theorem 3.12(1).

Let K be a field.

Definition 4.1 *An* abelian variety *A over K is a complete variety over K together with a group law $\mu : A \times A \longrightarrow A$ which is a morphism defined over K, and for which the inverse map $a \longmapsto a^{-1}$ is also a morphism defined over K.*

A morphism of abelian varieties is a morphism of varieties which is also a homomorphism of the underlying groups. The group law on an abelian variety is commutative (see [Lan83], Ch. II, §1, Theorem 1). Note that an abelian variety of dimension one is simply an elliptic curve. When $K = \mathbb{C}$, the classical uniformization of elliptic curves $E/\mathbb{C}$ may be generalized to abelian varieties $A/\mathbb{C}$ of arbitrary dimension g. A *lattice* Λ of $\mathbb{C}^g$ is a free $\mathbb{Z}$-module of rank $2g$ which has a basis which is also an $\mathbb{R}$-basis for $\mathbb{C}^g$.

Theorem 4.2 *Let $A/\mathbb{C}$ be an abelian variety of dimension g. There exists a lattice Λ of $\mathbb{C}^g$ and a complex analytic group isomorphism*

$$\phi : \mathbb{C}^g/\Lambda \longrightarrow A(\mathbb{C}).$$

Proof: See [Mum70], Ch. I, §1(2). □

We now describe how to associate an abelian variety $\mathrm{Jac}(C)/K$ to any complete nonsingular curve C/K of genus $g > 0$. A *divisor* D on C is a formal finite sum of $\overline{K}$-rational points on C, that is $D = \sum_{P \in C(\overline{K})} n_P P$, where each $n_P \in \mathbb{Z}$ and $n_P = 0$ for almost all $P \in C(\overline{K})$. We write $\mathrm{Div}(C)$ for the abelian group of divisors on C, where the sum of two divisors $D_1 = \sum_{P \in C(\overline{K})} n_P P$ and $D_2 = \sum_{P \in C(\overline{K})} m_P P$ is given by

$$D_1 + D_2 = \sum_{P \in C(\overline{K})} (n_P + m_P) P.$$

Given a rational function $f \in \overline{K}(C)^\times$, we define the divisor (f) of f to be $(f) = \sum_{P \in C(\overline{K})} \mathrm{ord}_P(f) P$, where $\mathrm{ord}_P(f)$ is the order of vanishing of f at P. A divisor on C is said to be *principal* if it is the divisor of some $f \in \overline{K}(C)^{\times}$, and the subgroup of $\mathrm{Div}(C)$ consisting of all principal divisors is denoted by $\mathrm{Pr}(C)$. Two divisors $D_1, D_2 \in \mathrm{Div}(C)$ are said to be *linearly equivalent* if $D_1 - D_2 \in \mathrm{Pr}(C)$. The group of linear equivalence classes of divisors on C is called the *Picard group* of C, and is denoted $\mathrm{Pic}(C)$; thus

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{Pr}(C).$$

Given any divisor $D = \sum_{P \in C(\overline{K})} n_P P$ on C, the *degree* $\deg(D)$ of D is defined to be $\deg(D) = \sum_{P \in C(\overline{K})} n_P$. The group $\mathrm{Pr}(C)$ is contained in the subgroup $\mathrm{Div}^0(C)$ of $\mathrm{Div}(C)$ consisting of the divisors of degree zero (see [Har97], Ch. II, Corollary 6.10), and thus we may define the degree zero part of the Picard group to be $\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{Pr}(C)$.

The absolute Galois group G_K of K acts naturally on $\mathrm{Div}(C)$ by

$$\sigma\left(\sum_{P \in C(\overline{K})} n_P P\right) = \sum_{P \in C(\overline{K})} n_P \sigma(P)$$

for $\sigma \in G_K$. Furthermore, for any $\sigma \in G_K$, two divisors D_1 and D_2 are linearly equivalent if and only if $\sigma(D_1)$ and $\sigma(D_2)$ are. Thus the action of G_K on $\mathrm{Div}(C)$ induces actions on $\mathrm{Pic}(C)$ and $\mathrm{Pic}^0(C)$.

For any $P \in C(\overline{K})$, let

$$f^P : C(\overline{K}) \longrightarrow \mathrm{Pic}^0(C)$$

be the map which takes $Q \in C(\overline{K})$ to the linear equivalence class $[Q - P]$ of

$Q - P$.

Theorem 4.3 *The group* $\mathrm{Pic}^0(C)$ *can be given the structure of the* $\overline{K}$*-rational points of an abelian variety* $\mathrm{Jac}(C)/K$ *of dimension equal to the genus of* C *in such a way that for each* $P \in C(\overline{K})$, f^P *is an embedding, and* $\mathrm{Jac}(C)$ *satisfies the following universal property: if* $\phi : C \longrightarrow A$ *is a morphism from* C *to an abelian variety* A *such that* $\phi(P) = 0$, *then there is a unique morphism of abelian varieties* $\psi : \mathrm{Jac}(C) \longrightarrow A$ *such that the diagram*

$$\begin{tikzcd} C \arrow[r, "f^P"] \arrow[dr, "\phi"'] & \mathrm{Jac}(C) \arrow[d, "\psi"] \\ & A \end{tikzcd}$$

commutes.

Proof: See [Mil86b], Proposition 2.3, Proposition 6.1, and Theorem 1.1. □

The abelian variety $\mathrm{Jac}(C)$ is called the *Jacobian* of C. The universal property of the Jacobian shows that assigning to a curve its Jacobian defines both a covariant and a contravariant functor from the category of complete nonsingular curves with nonconstant morphisms to that of abelian varieties. Given complete nonsingular curves C_1 and C_2, and a nonconstant morphism $\phi : C_1 \longrightarrow C_2$, the map $f^{\phi(P_0)} \circ \phi : C_1 \longrightarrow \mathrm{Jac}(C_2)$ satisfies $f^{\phi(P_0)} \circ \phi(P_0) = 0$ for each $P_0 \in C_1$. The universal property of $\mathrm{Jac}(C_1)$ gives a morphism of abelian varieties $\phi_* : \mathrm{Jac}(C_1) \longrightarrow \mathrm{Jac}(C_2)$. In terms of divisors, ϕ_* is given by

$$\phi_* : \left[\sum n_P P\right] \longmapsto \left[\sum n_P \phi(P)\right].$$

In particular, ϕ_* is independent of the choice of P_0 above. On the other hand, for each $Q \in C_2$, let $e_\phi(Q)$ denote the ramification index of ϕ at Q. Fixing a point $Q_0 \in C_2$, there is a morphism $f_\phi : C_2 \longrightarrow \mathrm{Jac}(C_1)$ given by

$$f_\phi : Q \longmapsto \left[\sum_{P \in \phi^{-1}(Q)} e_\phi(Q) P \; - \sum_{P \in \phi^{-1}(Q_0)} e_\phi(Q_0) P \right]$$

which satisfies $f_\phi(Q_0) = 0$. The universal property of $\mathrm{Jac}(C_2)$ gives a morphism of abelian varieties $\phi^* : \mathrm{Jac}(C_2) \longrightarrow \mathrm{Jac}(C_1)$, which is given in terms of divisors by

$$\phi^* : \left[\sum_{Q \in C_2} n_Q Q \right] \longmapsto \left[\sum_{Q \in C_2} n_Q \sum_{P \in \phi^{-1}(Q)} e_\phi(Q) P \right].$$

Once again, ϕ^* is seen to be independent of the choice of Q_0 above.

4.2 Tate Modules and ℓ-adic Representations

Let A/K be an abelian variety of dimension g, and fix a prime ℓ not equal to the characteristic of K. For each integer $m \in \mathbb{Z}$, there is an endomorphism $[m] : A(\overline{K}) \longrightarrow A(\overline{K})$ of A defined over K given by multiplication by m. We write $A[m] := \ker[m]$, and call the elements of $A[m]$ the *m-torsion points* of A. For each positive integer m not divisible by the characteristic of K, we have $\deg[m] = m^{2g}$ (see [Mil86a], Theorem 8.2). Applying this equality to every positive integer d dividing m shows that $A[m]$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{2g}$. As m ranges through powers of ℓ, the ℓ^n-torsion points together with the multiplication-by-ℓ maps $[\ell] : A[\ell^{n+1}] \longrightarrow A[\ell^n]$ form a directed system of groups. The inverse limit

$$T_\ell(A) := \varprojlim_{n \in \mathbb{N}} A[\ell^n]$$

is called the *(ℓ-adic) Tate module* of A. The Tate module $T_\ell(A)$ is naturally a free $\mathbb{Z}_\ell$-module of rank $2g$, where the action of $\alpha \in \mathbb{Z}_\ell$ on $A[\ell^n]$ is given by multiplication by the reduction of $\alpha \mod \ell^n$. This action preserves compatibility under the multiplication-by-ℓ maps, and thus defines an action of $\mathbb{Z}_\ell$ on $T_\ell(A)$.

Since the addition law on A is defined over K, the action of G_K on A commutes with $[m]$. Thus restricting to $A[m]$ gives an action of G_K on $A[m]$. Moreover, since this action commutes with the multiplication-by-ℓ map, we obtain a $\mathbb{Z}_\ell$-linear action of G_K on $T_\ell(A)$. Choosing a $\mathbb{Z}_\ell$-basis for $T_\ell(A)$ gives a homomorphism

$$\rho_\ell : G_K \longrightarrow \mathrm{GL}_{2g}(\mathbb{Z}_\ell),$$

called the *ℓ-adic representation associated to A.*

We define the *extended Tate module* $V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, which is a $\mathbb{Q}_\ell$-vector space of dimension $2g$, together with a $\mathbb{Q}_\ell$-linear action of G_K. This action gives a representation

$$\rho_\ell : G_K \longrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell),$$

which may be obtained from the ℓ-adic representation by extending scalars to $\mathbb{Q}_\ell$.

Let $\psi : A \longrightarrow B$ be a morphism of abelian varieties. Since ψ is a group homomorphism, it maps ℓ^n-torsion points of A to ℓ^n-torsion points of B, and commutes with the multiplication-by-ℓ maps on each side. Thus ψ induces a $\mathbb{Z}_\ell$-module homomorphism

$$\psi_\ell : T_\ell(A) \longrightarrow T_\ell(B)$$

by applying ψ componentwise, that is, $\psi_\ell : (a_n)_{n\in\mathbb{N}} \longmapsto (\psi_\ell(a_n))_{n\in\mathbb{N}}$, where $a_n \in A[\ell^n]$ and $[\ell]a_n = a_{n-1}$ for each positive integer n. We will also write ψ_ℓ for the map $V_\ell(A) \longrightarrow V_\ell(B)$ obtained by tensoring with $\mathbb{Q}_\ell$.

Proposition 4.4 *Let $\phi : C_1 \longrightarrow C_2$ be a nonconstant morphism of complete nonsingular curves defined over K, and let $\phi_\ell^* : T_\ell\left(\mathrm{Jac}(C_2)\right) \longrightarrow T_\ell\left(\mathrm{Jac}(C_1)\right)$ denote the map induced from $\phi^* : \mathrm{Jac}(C_2) \longrightarrow \mathrm{Jac}(C_1)$. Then ϕ_ℓ^* is injective.*

Proof: Let $\tilde{\phi}^* : \mathrm{Div}(C_2) \longrightarrow \mathrm{Div}(C_1)$ denote the map given by

$$\tilde{\phi}^* : \sum_{Q\in C_2} n_Q Q \longmapsto \sum_{Q\in C_2} n_Q \sum_{P\in\phi^{-1}(Q)} e_\phi(Q)P.$$

Suppose that $D \in \mathrm{Div}^0(C_2)$ is such that $\tilde{\phi}^*(D) = (f)$ for some $f \in \overline{K}(C_1)$. The map ϕ induces an injection of function fields $\overline{K}(C_2) \hookrightarrow \overline{K}(C_1)$, and we have

$$\mathrm{Norm}^{\overline{K}(C_1)}_{\overline{K}(C_2)}(f) = \deg\phi \cdot D.$$

In particular, the image of D in $\mathrm{Pic}^0(C_2) \cong \mathrm{Jac}(C_2)$ is a $\deg\phi$-torsion point. If $t \in T_\ell\left(\mathrm{Jac}(C_2)\right)$ is such that $\phi_\ell^*(t) = 0$, then every component of t is a degϕ-torsion point, and thus t is itself a degϕ-torsion point of $T_\ell\left(\mathrm{Jac}(C_2)\right)$. Since $T_\ell\left(\mathrm{Jac}(C_2)\right)$ is a free $\mathbb{Z}_\ell$-module, we must have $t = 0$. $\square$

Remark: Since $\mathbb{Q}_\ell$ is flat over $\mathbb{Z}_\ell$ (see [Lan93], Ch. XVI, Proposition 3.2), the map $\phi_\ell^* : V_\ell\left(\mathrm{Jac}(C_2)\right) \longrightarrow V_\ell\left(\mathrm{Jac}(C_1)\right)$ is also injective.

4.3 Reduction of Curves

Let K be a field of characteristic zero, C/K a complete nonsingular curve of genus $g > 0$, and $\mathfrak{p}$ a valuation ideal of K with corresponding valuation ring R. For any valuation ideal $\hat{\mathfrak{p}}$ of $\overline{K}$ above $\mathfrak{p}$, the action of the inertia group $I\left(\hat{\mathfrak{p}}/\mathfrak{p}\right)$ on the Jacobian of C is closely related to the reduction type of C at $\mathfrak{p}$.

Definition 4.5 *A K-*model *M of a variety V/K is a set of equations with coefficients in K, taken up to multiplication of each equation by elements of $K^\times$, such that M defines an element of the K-isomorphism class given by V.*

A particular set of equations in the equivalence class M will be called a *defining set of equations for M*. We will say that a defining set of equations for M is $\mathfrak{p}$-*reducible* if all of its coefficients lie in R, and each equation has at least one coefficient not in $\mathfrak{p}$. The *reduction* $\bar{M}$ of M at $\mathfrak{p}$ is the variety defined over the residue field $k = R/\mathfrak{p}$ obtained by reducing mod $\mathfrak{p}$ the coefficients of a $\mathfrak{p}$-reducible set of equations for M. Fixing a valuation ideal $\hat{\mathfrak{p}}$ of $\overline{K}$ above $\mathfrak{p}$ with valuation ring $\hat{R}$, we obtain a *reduction map* $r : M(\overline{K}) \longrightarrow \bar{M}(\overline{k})$ by choosing for each $\overline{K}$-rational point of M an expression which has projective coordinates in $\hat{R}$ but not all in $\hat{\mathfrak{p}}$, and reducing the coordinates mod $\hat{\mathfrak{p}}$.

Definition 4.6 *The curve C/K of genus g is said to have* good reduction *at $\mathfrak{p}$ if it has a K-model whose reduction at $\mathfrak{p}$ is a nonsingular curve of genus g. An abelian variety A/K of dimension g is said to have good reduction at $\mathfrak{p}$ if it has a K-model whose reduction at $\mathfrak{p}$ is an abelian variety of dimension g.*

If C (respectively A) has good reduction at $\mathfrak{p}$, we will often identify C (resp. K) with a K-model whose reduction is as in Definition 4.6. In this case, the reduced curve (respectively reduced abelian variety) is independent of the choice of such a K-model. If C or A does not have good reduction at $\mathfrak{p}$, then we say that it has *bad reduction* at $\mathfrak{p}$.

Jacobians are well-behaved with respect to good reduction in the sense that if C has good reduction at $\mathfrak{p}$ then so does $\mathrm{Jac}(C)$, and in this case, the Jacobian of the reduction of C is the reduction of $\mathrm{Jac}(C)$. The converse, however, is not true; there exist curves with bad reduction at a valuation ideal $\mathfrak{p}$ whose Jacobians have good reduction at $\mathfrak{p}$ (see [Maz86], p.238 for an example).

Definition 4.7 *A representation ρ of G_K is said to be* unramified *at $\mathfrak{p}$ if $\rho\left(I\left(\hat{\mathfrak{p}}/\mathfrak{p}\right)\right) = 1$ for each valuation ideal $\hat{\mathfrak{p}}$ of $\overline{K}$ above $\mathfrak{p}$. Equivalently, ρ is unramified at $\mathfrak{p}$ if $\mathfrak{p}$ is unramified in the extension of K corresponding to the quotient $G_K/\ker(\rho)$.*

Proposition 4.8 *Let ℓ be a rational prime not below $\mathfrak{p}$. If the abelian variety A/K has good reduction at $\mathfrak{p}$, then the ℓ-adic representation ρ_ℓ attached to A is unramified at $\mathfrak{p}$.*

Proof: It suffices to show that the representation $\bar{\rho}_{\ell^n} : G_K \longrightarrow \mathrm{Aut}(A[\ell^n])$ describing the action of G_K on the ℓ^n-torsion points of A is unramified for each n. Let $\bar{A}$ denote the reduction of A at $\mathfrak{p}$, and let $\hat{\mathfrak{p}}$ be any valuation ideal of $\overline{K}$ above $\mathfrak{p}$. The reduction map restricts to an isomorphism

$$A[\ell^n]^{I(\hat{\mathfrak{p}}/\mathfrak{p})} \xrightarrow{\cong} \bar{A}[\ell^n]$$

(see [ST68], §1, Lemma 2). Since $A[\ell^n]$ and $\bar{A}[\ell^n]$ are both free $\mathbb{Z}/\ell^n\mathbb{Z}$-modules of rank $2\dim\bar{A} = 2\dim A$, counting gives $A[\ell^n]^{I(\hat{\mathfrak{p}}/\mathfrak{p})} = A[\ell^n]$. □

Remark: The converse to Proposition 4.8 is also true, and is known as the criterion of Néron-Ogg-Shafarevich. To be precise, if ρ_ℓ is unramified at $\mathfrak{p}$ for some ℓ not below $\mathfrak{p}$, then A has good reduction at $\mathfrak{p}$ (see [ST68], §1).

4.4 Mumford Curves

When a curve C/K has a special type of bad reduction at $\mathfrak{p}$, strong information can be obtained about the action of the inertia groups above $\mathfrak{p}$ on the Tate module of the Jacobian of C. To make this precise, it will be useful to have an alternative description of the inertia group. Let K and F be fields, and let $\phi : K \longrightarrow F \cup \{\infty\}$ be a nontrivial place of K with valuation ring R and valuation ideal $\mathfrak{p}$, as in §2.2. Let $K_\mathfrak{p}$ denote the completion of K at $\mathfrak{p}$, which is the quotient field of the completion of R with respect to the $\mathfrak{p}$-adic topology. Let L be a Galois extension of K, $\hat{\mathfrak{p}}$ a valuation ideal of L above $\mathfrak{p}$, and $L_{\hat{\mathfrak{p}}}$ the completion of L at $\hat{\mathfrak{p}}$. The extension $L_{\hat{\mathfrak{p}}}/K_\mathfrak{p}$ is Galois.

Proposition 4.9 *The map* $r_L : \mathrm{Gal}\left(L_{\hat{\mathfrak{p}}}/K_\mathfrak{p}\right) \longrightarrow \mathrm{Gal}\left(L/K\right)$ *given by restriction to L defines an isomorphism of* $\mathrm{Gal}\left(L_{\hat{\mathfrak{p}}}/K_\mathfrak{p}\right)$ *onto the decomposition group* $D\left(\hat{\mathfrak{p}}/\mathfrak{p}\right)$.

Proof: See [Ser68], Ch. II, §3, Corollaire 4. □

Now let $K = k(t)$, where k is an algebraically closed subfield of $\mathbb{C}$. For each $P \in \mathbb{P}^1(k)$, let $\phi_P : K \longrightarrow k \cup \{\infty\}$ be the place given by $\phi_P(f) = f(P)$ for $f \in K$ (see §2.2). Identifying $\mathbb{P}^1(k)$ with $k \cup \{\infty\}$, the completion K_P of K with respect to ϕ_P is given by

$$K_P = \begin{cases} k((t-P)) & \text{if } P \in k, \\ k((\frac{1}{t})) & \text{if } P = \infty. \end{cases}$$

Let $\mathfrak{p}$ be the valuation ideal of K at P, and $\hat{\mathfrak{p}}$ a valuation ideal of $\overline{K}$ above $\mathfrak{p}$. Then $I(\hat{\mathfrak{p}}/\mathfrak{p}) = D(\hat{\mathfrak{p}}/\mathfrak{p})$ may be identified with $\mathrm{Gal}\left(\overline{K}_P/K_P\right)$ as in Proposition 4.9. Moreover, we have

$$\overline{K}_P = \begin{cases} \bigcup_{n\in\mathbb{N}} k\left(\left((t-P)^{1/n}\right)\right) & \text{if } P \in k \\ \bigcup_{n\in\mathbb{N}} k\left(\left((\frac{1}{t})^{1/n}\right)\right) & \text{if } P = \infty. \end{cases}$$

Understanding the action of the inertia group $I(\hat{\mathfrak{p}}/\mathfrak{p})$ on the $\overline{K}$-rational points of an abelian variety A/K is equivalent to understanding the Galois action on the $\overline{K_P}$-rational points of A (as a variety over K_P).

Definition 4.10 *A complete nonsingular curve C/K_P is called a* Mumford curve *if it has a K_P-model whose reduction (at P) is a union of projective lines whose only singularities are ordinary double points.*

Mumford proved the existence of the following uniformization, generalizing a theorem of Tate in the case of elliptic curves.

Theorem 4.11 *Let C/K_P be a Mumford curve of genus g, and J its Jacobian. Then there is a surjective group homomorphism*

$$\upsilon : (\overline{K}_P^{\times})^g \longrightarrow J\left(\overline{K}_P\right)$$

commuting with the action of G_{K_P} on each side, whose kernel is a discrete subgroup of $(\overline{K}_P^{\times})^g$ freely generated by elements $q_1, \ldots, q_g \in \left(K_P^{\times}\right)^g$.

Proof: See [Gv80], Ch. VI, §§1.3,1.4. That a Mumford curve in our sense is indeed a Mumford curve in the sense of [Gv80] may be found in [Gv80], Ch. IV, Theorem 3.10. □

Remark: Theorem 4.11 remains true if K_P is replaced with any field which is complete with respect to a non-archimedean valuation.

Let $\mathfrak{p}$ and $\hat{\mathfrak{p}}$ be as above. Let ℓ be a rational prime, and let ρ_ℓ be the ℓ-adic representation associated to the Jacobian of a curve C/K of genus g.

Corollary 4.12 *Suppose that C becomes a Mumford curve over K_P. Then for each $\sigma \in I\left(\hat{\mathfrak{p}}/\mathfrak{p}\right)$, we have*

$$\rho_\ell(\sigma) \sim \begin{pmatrix} \mathrm{Id}_g & * \\ 0 & \mathrm{Id}_g \end{pmatrix},$$

where Id_g denotes the $g \times g$ identity matrix.

Proof: Since the isomorphism υ of Theorem 4.11 commutes with the action of G_{K_P}, it suffices to consider the action of G_{K_P} on the ℓ^nth roots of the identity in $(\overline{K}_P^{\times})^g/\langle q_1, \ldots, q_g\rangle$. Choosing a primitive ℓ^nth root of unity $\zeta_n \in \overline{K}_P$, the subgroup of ℓ^nth roots of the identity in $(\overline{K}_P^{\times})^g/\langle q_1, \ldots, q_g\rangle$ is generated by the cosets of $(\zeta_n, 1, \ldots, 1), (1, \zeta_n, 1, \ldots, 1), \ldots, (1, \ldots, 1, \zeta_n)$, together with ℓ^nth roots of $q_1, \ldots, q_g$. Fix ℓ^nth roots $q_1^{1/\ell^n}, \ldots, q_g^{1/\ell^n}$ of $q_1, \ldots, q_g$. Each $\sigma \in G_{K_P}$ fixes each of $(\zeta_n, 1, \ldots, 1), \ldots, (1, \ldots, 1, \zeta_n)$, and since each q_j is an element of $\left(K_P^\times\right)^g$, σ takes q_j^{1/ℓ^n} to another ℓ^nth root of q_j. Hence

$$\sigma q_j^{1/\ell^n} = (\zeta_n^{j_1}, \ldots, \zeta_n^{j_g}) q_j^{1/\ell^n}$$

for some $j_1, \ldots, j_g \in \mathbb{Z}/\ell^n\mathbb{Z}$. Therefore, with respect to the $\mathbb{Z}/\ell^n\mathbb{Z}$-basis $\{(\zeta_n, 1, \ldots, 1), \ldots, (1, \ldots, 1, \zeta_n), q_1, \ldots, q_g\}$ for the ℓ^nth roots of the identity in $(\overline{K}_P^\times)^g / \langle q_1, \ldots, q_g \rangle$, σ acts as $\begin{pmatrix} \mathrm{Id}_g & * \\ 0 & \mathrm{Id}_g \end{pmatrix}$. The result now follows from the discussion preceding Theorem 4.11. $\square$

4.5 Hypergeometric Families of Curves

Fix an odd prime p, and consider the so-called hypergeometric family of curves over $\mathbb{Q}(t)$ given by

$$C_n : y^2 = x\left(x^{2p^n} + (4t-2)x^{p^n} + 1\right)$$

for each $n \geq 0$. Let ζ_n be a generator of the group μ_{p^n} of p^nth roots of unity in $\overline{\mathbb{Q}}$. The group μ_{p^n} acts as a group of automorphisms on C_n by

$$\zeta_n \cdot (x, y) = (\zeta_n x, \zeta_n^{\frac{p^n+1}{2}} y).$$

We will denote by γ_n the automorphism of C_n given by the action of ζ_n in order to distinguish the group ring $\mathbb{Z}_p[\gamma_n] = \mathbb{Z}_p[\mu_{p^n}]$ from the subring $\mathbb{Z}_p[\zeta_n]$ of the field $\mathbb{Q}_p(\zeta_n)$. We will also identify μ_{p^n} with the automorphism group generated by γ_n.

In addition to the hyperelliptic involution $(x, y) \longmapsto (x, -y)$ and the action of μ_{p^n}, there is also an involution τ_n of C_n given by

$$\tau_n : (x, y) \longmapsto \left(\frac{1}{x}, \frac{y}{x^{p^n+1}}\right).$$

Note that $\tau_n \circ \gamma_n = \gamma_n^{-1} \circ \tau_n$, so the automorphism group $\langle \tau_n, \gamma_n \rangle$ is isomorphic to the dihedral group of order $2p^n$. Tautz, Top, and Verberkmoes studied C_n and its quotient $C_n^- = C_n/\langle \tau_n \rangle$ in [TTV91] (see in particular Theorem 1 and Proposition 3). For any odd prime r, the Galois representation on the r-torsion points of the Jacobian of C_1^- was subsequently studied by Darmon in connection with the equation $x^r + y^r = z^p$ (see [Dar00], Theorem 1.10), as well as by Darmon and Mestre to construct a regular extension of $\mathbb{Q}(\zeta_n + \zeta_n^{-1})(t)$ with Galois group $\mathrm{PSL}_2(\mathbb{F}_q)$ for certain finite fields $\mathbb{F}_q$ (see [DM00], §§2,3).

Proposition 4.13 *The quotient curve C_n^- is birationally equivalent over $\mathbb{Q}(t)$ to the curve given by*

$$y^2 = x g_n(x^2 - 2) + 4t - 2,$$

where $g_n(x) = \prod_{j=1}^{\frac{p^n-1}{2}} (x + \zeta_n^j + \zeta_n^{-j})$.

Idea of Proof: The subfield of the function field of C_n consisting of those elements fixed by τ_n is generated by $x + x^{-1}$ and $\frac{y}{x^{\frac{p^n+1}{2}}}$. Using the formal relation

$$X^{p^n} + X^{-p^n} = (X + X^{-1}) g_n(X^2 + X^{-2}) \tag{4.14}$$

gives the desired equation. See [TTV91], Proposition 3 for details. $\square$

For each $m \leq n$, there is a morphism $\phi_{n,m} : C_n \longrightarrow C_m$ given by

$$\phi_{n,m} : (x, y) \longmapsto \left(x^{p^{n-m}}, x^{\frac{p^{n-m}-1}{2}} y \right).$$

If the generators ζ_n for each μ_{p^n} are chosen to be compatible in the sense that $\zeta_n^p = \zeta_{n-1}$ for all n, then $\phi_{n,m} \circ \gamma_n = \gamma_m \circ \phi_{n,m}$. Also, each $\phi_{n,m}$ satisfies $\tau_m \circ \phi_{n,m} = \phi_{n,m} \circ \tau_n$, so $\phi_{n,m}$ induces a morphism $\phi^-_{n,m} : C^-_n \longrightarrow C^-_m$ given explicitly by composing the maps

$$\phi^-_{n,n-1} : (x, y) \longrightarrow \left(\frac{1}{2^{p-1}} \sum_{k=0}^{p-1} \binom{p}{2k} x^{p-2k} (x^2 - 4)^k,\ y \right).$$

Note that the action of the Galois group $G_{\mathbb{Q}(t)}$ commutes with the maps $\phi_{n,m}, \phi^-_{n,m}$. Letting J_n and J^-_n denote the Jacobians of C_n and C^-_n respectively, the induced maps $(\phi_{n,m})_* : V_p(J_n) \longrightarrow V_p(J_m)$ make the extended Tate modules into a compatible system of $G_{\mathbb{Q}(t)}$-modules (similarly for $V_p(J^-_n)$ with the maps $(\phi^-_{n,m})_*$).

Since γ_n does not commute with τ_n, it does not give rise to an automorphism of C^-_n. However, the endomorphism $\gamma_n + \gamma_n^{-1}$ of J_n does commute with τ_n, and gives rise to endomorphisms of J^-_n. Let $\pi_n : C_n \longrightarrow C^-_n$ be the natural map. From the proof of Proposition 4.4, the kernel of $\pi^*_n : J^-_n \longrightarrow J_n$ is contained in $J^-_n[\deg \pi_n] = J^-_n[2]$.

Proposition 4.15 *For each $\gamma \in \mu_{p^n}$, there is an endomorphism $(\gamma + \gamma^{-1})^-$ of J^-_n such that $\pi^*_n \circ (\gamma + \gamma^{-1})^- = (\gamma + \gamma^{-1})|_{\mathrm{Im}\pi^*_n}$.*

Proof: See [TTV91], §3.1. $\square$

When it is clear from the context that we are referring to endomorphisms of J_n^-, we will write $\gamma + \gamma^{-1}$ in place of $(\gamma + \gamma^{-1})^-$.

The action of the full Galois group $G_{\mathbb{Q}(t)}$ does not commute with the action of μ_{p^n}; however, if we restrict to the subgroup $G_{\mathbb{Q}(\mu_{p^\infty},t)}$, then these actions do commute, so the action of $G_{\mathbb{Q}(\mu_{p^\infty},t)}$ on $V_p(J_n)$ is $\mathbb{Q}_p[\mu_{p^n}]$-linear. In order to obtain 2-dimensional representations of $\Pi_{\mathbb{Q}(\mu_{p^\infty})}$ on $V_p(J_n)$, we must show that $V_p(J_n)$ is a free $\mathbb{Q}_p[\mu_{p^n}]$-module of rank two. First we will show that if $V_p(J_n)$ is indeed a free $\mathbb{Q}_p[\mu_{p^n}]$-module, then it must have rank two.

Proposition 4.16 *The dimension of J_n is p^n, and the dimension of J_n^- is $\frac{p^n-1}{2}$.*

Proof: Since the dimension of the Jacobian of a curve is equal to the genus of the curve, we must calculate the genera of C_n and C_n^-. Both may be computed using the Riemann-Hurwitz formula. For example, let

$$h : C_n\left(\overline{\mathbb{Q}(t)}\right) \longrightarrow \mathbb{P}^1\left(\overline{\mathbb{Q}(t)}\right)$$

be the degree two map taking (x, y) to x. Then h is ramified only at ∞ and the roots of $x\left(x^{2p^n} + (4t-2)x^{p^n} + 1\right)$, which are distinct. Thus h has $2p^n+2$ ramification points, each having index two, so the Riemann-Hurwitz formula gives

$$2\,\mathrm{genus}(C_n) - 2 = 2\left(2\,\mathrm{genus}(\mathbb{P}^1) - 2\right) + 2p^n + 2,$$

and therefore, $\mathrm{genus}(C_n) = p^n$. $\square$

To show that $V_p(J_n)$ is free over $\mathbb{Q}_p[\mu_{p^n}]$, we will need the following lemmas:

Lemma 4.17 *Let K be a field whose characteristic is not equal to p, and let C/K be a curve with Jacobian J. Suppose that ξ is a nontrivial automorphism of C having a fixed point $P_\xi \in C$. Then the automorphism of $T_p(J)$ induced from ξ is also nontrivial.*

Proof: Let $f^{P_\xi} : C \longrightarrow J$ be the embedding of Theorem 4.3. For any point $Q \in C$ not fixed by ξ, we have

$$\xi f^{P_\xi}(Q) = \xi_*[Q - P_\xi] = [\xi_* Q] - [P_\xi] = f^{P_\xi}(\xi Q),$$

and $f^{P_\xi}(\xi Q) \neq f^{P_\xi}(Q)$ since f^{P_ξ} is injective. Therefore ξ_* is a nontrivial automorphism of J. The result now follows from the fact that for any abelian varieties A and B over a field K of characteristic not equal to p, the natural map

$$\mathrm{Hom}(A, B) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p-\mathrm{mod}}(T_p(A), T_p(B))$$

is injective (see [Mil86a], Lemma 12.2). $\square$

Lemma 4.18 *Let G be a finite group acting as automorphisms on a curve $C/\mathbb{C}(t)$ with Jacobian J. Then for some $\mathbb{Q}_p[G]$-module M, $V_p(J)$ is isomorphic to M^2 as a $\mathbb{Q}_p[G]$-module.*

Proof: Let $\alpha \in \mathbb{C}$ be a point at which C has good reduction, and let J_α denote the reduction of J at $t = \alpha$. Since $\mathrm{char}(\mathbb{C}) = 0$, for each $m \in \mathbb{N}$ the reduction map $r_\alpha : J \longrightarrow J_\alpha$ restricts to an isomorphism from the m-torsion points of J fixed by any given inertia group above $t = \alpha$ to the m-torsion points of J_α (see [ST68], Lemma 2). Since J has good reduction at $t = \alpha$, each inertia group above $t = \alpha$ acts trivially on $T_p(J)$, and therefore r_α induces an isomorphism $T_p(J) \cong T_p(J_\alpha)$. Thus it suffices to prove the result when J is replaced with J_α, where the action of G on J_α is induced from J via r_α.

Let g be the dimension of J_α, and let Λ be a lattice of $\mathbb{C}^g$ such that $\mathbb{C}^g/\Lambda \cong J_\alpha$ as in Theorem 4.2. The action of G on J_α lifts to a linear action on $\mathbb{C}^g$ fixing Λ. Let $\{\lambda_1, \dots, \lambda_{2g}\}$ be a $\mathbb{Z}$-basis for Λ. Reordering the λ_j's if necessary, we may assume that $\{\lambda_1, \dots, \lambda_g\}$ and $\{\lambda_{g+1}, \dots, \lambda_{2g}\}$ are $\mathbb{C}$-bases for $\mathbb{C}^g$. Since $\{\lambda_1 \otimes 1, \dots, \lambda_{2g} \otimes 1\}$ is a $\mathbb{C}$-basis for $\Lambda \otimes \mathbb{C}$, the representation of G on $\Lambda \otimes \mathbb{C}$ is isomorphic to two copies of that on $\mathbb{C}^g$.

On the other hand, identifying $J_\alpha[p^n]$ with $\frac{1}{p^n}\Lambda/\Lambda$, there is a canonical $\mathbb{Z}_p$-module isomorphism $T_p(J_\alpha) \cong \Lambda \otimes \mathbb{Z}_p$ commuting with the action of G, given by

$$\left(\sum_{j=1}^{2g} a_{j,n} \frac{\lambda_j}{p^n}\right)_{n\in\mathbb{N}} \longmapsto \sum_{j=1}^{2g} \lambda_j \otimes (a_{j,n})_{n\in\mathbb{N}},$$

where each $a_{j,n} \in \mathbb{Z}/p^n\mathbb{Z}$. Let χ_V be the character corresponding to the representation of G on $V := V_p(J_\alpha) \cong \mathbb{Q}_p^{2g}$, and χ_W the character corresponding to the representation of G on $W := \mathbb{C}^g$. From above, there is a $\mathbb{C}[G]$-module isomorphism $\Lambda \otimes \mathbb{C} \cong W^2$, so the character corresponding to the representation of G on $\Lambda \otimes \mathbb{C}$ is $2\chi_W$. Since G acts on the free $\mathbb{Z}$-module Λ, χ_W must take values in $\mathbb{Q}$, and thus $2\chi_W$ is the character obtained from the representation of G on $\Lambda \otimes \mathbb{Q}$, and hence also from that on $\Lambda \otimes \mathbb{Q}_p \cong V$. Therefore,

χ_V is equal to $2\chi_W$. $\square$

Proposition 4.19 *The extended Tate module $V_p(J_n)$ is a free module of rank two over $\mathbb{Q}_p[\mu_{p^n}]$.*

Proof: Let χ be an irreducible character of μ_{p^n} over $\mathbb{Q}_p$. Over $L = \mathbb{Q}_p(\zeta_n)$, χ decomposes as a sum of 1-dimensional characters $\chi_1, \dots, \chi_r$. The characters $\chi_1, \dots, \chi_r$ form a Galois conjugacy class over $\mathbb{Q}_p$, and each appears with multiplicity one (see [Isa94], Theorem 9.21). On the other hand, given any irreducible character $\tilde{\chi}$ of μ_{p^n} over L, there is a unique irreducible character χ of μ_{p^n} over $\mathbb{Q}_p$ which has $\tilde{\chi}$ as a constituent when lifted to L (see [Isa94], Corollary 9.7). Therefore, the irreducible characters χ of μ_{p^n} over $\mathbb{Q}_p$ are precisely those of the form

$$\chi = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_k)/\mathbb{Q}_p)} \tilde{\chi}^{\sigma},$$

where $\tilde{\chi}$ is a 1-dimensional character of μ_{p^n} over $\mathbb{Q}_p(\zeta_k)$ which is not defined over $\mathbb{Q}_p(\zeta_{k-1})$. Fixing a generator γ_n of μ_{p^n}, such a character $\tilde{\chi}$ is determined by $\tilde{\chi}(\gamma_n)$, which is a primitive p^kth root of 1. Moreover, if $\tilde{\chi}'$ is any other character of μ_{p^n} defined over $\mathbb{Q}_p(\zeta_k)$ but not over $\mathbb{Q}_p(\zeta_{k-1})$, then $\tilde{\chi}'(\gamma_n)$ is also a primitive p^kth root of 1, and hence there is some $\sigma \in \mathrm{Gal}\,(\mathbb{Q}_p(\zeta_k)/\mathbb{Q}_p)$ for which $\tilde{\chi}' = \tilde{\chi}^{\sigma}$. Therefore, the irreducible characters of μ_{p^n} over $\mathbb{Q}_p$ are in one-to-one correspondence with the factor groups of μ_{p^n}, and are given by $\chi_0, \dots, \chi_n$, where χ_0 is the trivial character, and χ_j has dimension $p^j - p^{j-1}$ for each $j = 1, \dots, n$.

When $n = 0$, $V_p(J_0)$ has rank two over $\mathbb{Q}_p$ by Proposition 4.16. Suppose for induction that $V_p(J_{n-1}) \cong \mathbb{Q}_p[\mu_{p^{n-1}}]^2$ as $\mathbb{Q}_p[\mu_{p^{n-1}}]$-modules. By Proposition 4.4, the map $\phi_{n,n-1} : C_n \longrightarrow C_{n-1}$ induces an injection

$$\left(\phi^*_{n,n-1}\right)_p : V_p(J_{n-1}) \hookrightarrow V_p(J_n).$$

Since γ_n acts on the image of $V_p(J_{n-1})$ as a generator γ_{n-1} of $\mu_{p^{n-1}}$, $\left(\phi^*_{n,n-1}\right)_p$ gives an inclusion $\mathbb{Q}_p[\mu_{p^{n-1}}]^2 \hookrightarrow V_p(J_n)$ of $\mathbb{Q}_p[\mu_{p^n}]$-modules. Since $\gamma_n^{p^{n-1}}$ acts nontrivially on C_n, by Lemma 4.17, the automorphism induced from $\gamma_n^{p^{n-1}}$ on $V_p(J_n)$ also acts nontrivially, and therefore μ_{p^n} acts faithfully on $V_p(J_n)$. From above, there is only one irreducible representation of μ_{p^n} over $\mathbb{Q}_p$ which does not factor through $\mu_{p^{n-1}}$, namely that having the character χ_n; therefore, the $\mathbb{Q}_p[\mu_{p^n}]$-module M corresponding to χ_n must appear as a summand of $V_p(J_n)$ (as a $\mathbb{Q}_p[\mu_{p^n}]$-module). By Lemma 4.18, two copies of M must appear, so there is an isomorphic copy of $\mathbb{Q}_p[\mu_{p^{n-1}}]^2 \oplus M^2$ contained in $V_p(J_n)$. Now $\mathbb{Q}_p[\mu_{p^{n-1}}] \oplus M$ is a direct sum of all irreducible $\mathbb{Q}_p[\mu_{p^n}]$-modules, and hence is isomorphic to $\mathbb{Q}_p[\mu_{p^n}]$. By Proposition 4.16, $V_p(J_n)$ has $\mathbb{Q}_p$-dimension $2p^n$, so the inclusion of $\mathbb{Q}_p[\mu_{p^n}]^2$ in $V_p(J_n)$ is an isomorphism. $\square$

Remark: For each choice of n-tuple

$$\boldsymbol{\zeta} = (1, \zeta_1, \ldots, \zeta_n) \in \{1\} \times \mu_p \times \cdots \times \mu_{p^n}$$

in which each ζ_j is a primitive p^jth root of unity in $\overline{\mathbb{Q}}_p$, there is a ring isomorphism

$$\mathbb{Q}_p[\mu_{p^n}] \cong \mathbb{Q}_p \oplus \mathbb{Q}_p(\zeta_1) \oplus \cdots \oplus \mathbb{Q}_p(\zeta_n)$$

given by mapping γ_n to $\boldsymbol{\zeta}$. This isomorphism arises through the isomorphism

$\mathbb{Q}_p[\mu_{p^n}] \cong \mathbb{Q}_p[T]/\left(T^{p^n}-1\right)$ which takes γ_n to T. Factoring $T^{p^n}-1$ and applying the Chinese remainder theorem gives the isomorphism above. Choosing a $\mathbb{Q}_p[\mu_{p^n}]$-basis for $V_p(J_n)$, we obtain an isomorphism

$$V_p(J_n) \cong \mathbb{Q}_p^2 \oplus \mathbb{Q}_p(\zeta_1)^2 \oplus \cdots \oplus \mathbb{Q}_p(\zeta_n)^2$$

of $\mathbb{Q}_p[\mu_{p^n}]$-modules.

By Proposition 4.4, we may view $V_p(J_n^-)$ and $V_p(J_k)$ as lying inside $V_p(J_n)$ whenever $k < n$.

Lemma 4.20 *The intersection of $V_p(J_n^-)$ with $V_p(J_0)$ in $V_p(J_n)$ is trivial.*

Proof: Since $\phi_{n,0}(P) = \phi_{n,0}(Q)$ if and only if $P = \gamma_n^j Q$ for some j, $V_p(J_0)$ is contained in the submodule $V_p(J_n)^{\mu_{p^n}}$ of elements of $V_p(J_n)$ fixed by μ_{p^n}. Similarly, $V_p(J_n^-)$ is contained in $V_p(J_n)^{\langle\tau_n\rangle}$. Now $\phi_{n,0} \circ \tau_n = \tau_0 \circ \phi_{n,0}$, so the action of τ_n on $V_p(J_n)$ restricts to the action of τ_0 on $V_p(J_0)$. Note that τ_0 acts nontrivially on every point $(x, y) \in C_0$ for which $x \neq \pm 1$, and fixes the points where $x = \pm 1$. By Lemma 4.17, $\langle\tau_0\rangle$ and hence also $\langle\tau_n\rangle$ act faithfully on $V_p(J_0)$. Let $D_n = \langle\gamma_n, \tau_n\rangle$, so that $V_p(J_n)^{D_n} = V_p(J_n)^{\mu_{p^n}} \cap V_p(J_n)^{\langle\tau_n\rangle}$. Suppose that $V_p(J_n)^{D_n}$ is nontrivial; then by Lemma 4.18, it has $\mathbb{Q}_p$-dimension at least two. On the other hand, by Proposition 4.19, $V_p(J_n)^{\mu_{p^n}}$ has $\mathbb{Q}_p$-dimension two, so we must have $V_p(J_n)^{D_n} = V_p(J_n)^{\mu_{p^n}}$, contradicting that $\langle\tau_n\rangle$ acts faithfully on $V_p(J_0) \subset V_p(J_n)^{\mu_{p^n}}$. $\square$

Proposition 4.21 *The $\mathbb{Q}_p$-vector space $V_n := V_p(J_n^-) \oplus V_p(J_0) \subset V_p(J_n)$ is a free $\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]$-module of rank two. Moreover, two elements $b_0, b_1 \in V_p(J_n)$ form a $\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]$-basis for V_n if and only if they are elements of V_n and they form a $\mathbb{Q}_p[\mu_{p^n}]$-basis for $V_p(J_n)$.*

Proof: Suppose that $\{b_0, b_1\} \subset V_n$ is a $\mathbb{Q}_p[\mu_{p^n}]$-basis for $V_p(J_n)$. Then the set $B = \{(\gamma_n^j + \gamma_n^{-j})b_l\}_{j=0,\dots,\frac{p^n-1}{2};\, l=0,1} \subset V_n$ is linearly independent over $\mathbb{Q}_p$, and thus generates a $\mathbb{Q}_p$-vector space of dimension $p^n + 1$ contained in V_n. By Proposition 4.16, V_n has $\mathbb{Q}_p$-dimension $2\left(\frac{p^n-1}{2}\right) + 2 = p^n + 1$, so B is a $\mathbb{Q}_p$-basis for V_n; in particular, b_0, b_1 generate V_n over $\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]$. Furthermore, since b_0, b_1 are linearly independent over $\mathbb{Q}_p[\mu_{p^n}]$, they must also be linearly independent over $\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]$. Therefore, $\{b_0, b_1\}$ forms a basis for V_n over $\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]$. Thus to prove the first statement it suffices to show that there exists a $\mathbb{Q}_p[\mu_{p^n}]$-basis $\{b_0, b_1\}$ for $V_p(J_n)$ which is contained in V_n.

Note that $D_n = \langle \gamma_n, \tau_n \rangle$ is isomorphic to the dihedral group of order $2p^n$. The irreducible characters of D_n over $\overline{\mathbb{Q}}$ consist of the trivial character, the nontrivial irreducible character of $D_n/\langle \tau_n \rangle$, and $\frac{p^n-1}{2}$ characters of dimension two each taking the value 0 at τ_n (see [JL93], §18.3). Since τ_n has order 2, it must have eigenvalues 1 and -1 under each of the two-dimensional irreducible representations. From Lemma 4.20, the representation of D_n on $V_p(J_0) = V_p(J_n)^{\mu_{p^n}}$ consists of two copies of the nontrivial one-dimensional representation. Each irreducible summand of the representation of D_n on $V_p(J_n)/V_p(J_0)$ decomposes over $\overline{\mathbb{Q}}_p$ as a sum of the two-dimensional representations of D_n, and the subspace of τ_n-fixed points of each of these has dimension one. Thus the subspace $(V_p(J_n)/V_p(J_0))^{\tau_n}$ of $V_p(J_n)/V_p(J_0)$ has dimension $\frac{2p^n-2}{2} = p^n - 1$, and contains $V_p(J_n^-)$. Since $V_p(J_n^-)$ itself has dimension $p^n - 1$, we have $V_p(J_n^-) = V_p(J_n)^{\tau_n}$. Now

$$V_p(J_{n-1}) \cap V_p(J_n^-) = V_p(J_{n-1})^{\tau_n} = V_p(J_{n-1})^{\tau_{n-1}} = V_p(J_{n-1}^-),$$

so $V_p(J_n^-) \cap V_n = V_{n-1}$. Fix a $\mathbb{Q}_p[\mu_{p^n}]$-module isomorphism

$$V_p(J_n) \cong \mathbb{Q}_p^2 \oplus \mathbb{Q}_p(\zeta_1)^2 \oplus \cdots \oplus \mathbb{Q}_p(\zeta_n)^2,$$

and identify each subspace with its image in $\mathbb{Q}_p^2 \oplus \cdots \oplus \mathbb{Q}_p(\zeta_n)^2$. Since $V_p(J_{n-1}) = \mathbb{Q}_p^2 \oplus \cdots \oplus \mathbb{Q}_p(\zeta_{n-1})^2$, we have $V_n = V_{n-1} \oplus (\mathbb{Q}_p(\zeta_n)^2 \cap V_n)$ as a $\mathbb{Q}_p$-vector space, and hence

$$\dim_{\mathbb{Q}_p} \left(\mathbb{Q}_p(\zeta_n)^2 \cap V_n\right) = \dim_{\mathbb{Q}_p} V_n - \dim_{\mathbb{Q}_p} V_{n-1} = p^n - p^{n-1}.$$

We now proceed by induction. When $n = 0$, $V_0 = V_p(J_0)$, and therefore contains a $\mathbb{Q}_p$-basis for $V_p(J_0)$. Suppose for induction that V_{n-1} contains a $\mathbb{Q}_p[\mu_{p^{n-1}}]$-basis $\{b_{0,n-1}, b_{1,n-1}\}$ for $V_p(J_{n-1})$. If $(\mathbb{Q}_p(\zeta_n)^2 \cap V_n)$ contains a $\mathbb{Q}_p(\zeta_n)$-basis $\{b_{0,n}, b_{1,n}\}$ for $\mathbb{Q}_p(\zeta_n)^2$, then $\{b_{0,n} + b_{0,n-1}, b_{1,n} + b_{1,n-1}\}$ is a $\mathbb{Q}_p[\mu_{p^n}]$-basis for $V_p(J_n)$ contained in V_n, as desired. If not, then since

$$\dim_{\mathbb{Q}_p} \left(\mathbb{Q}_p(\zeta_n)^2 \cap V_n\right) = p^n - p^{n-1} = \dim_{\mathbb{Q}_p} \mathbb{Q}_p(\zeta_n),$$

there must be some $b \in \mathbb{Q}_p(\zeta_n)^2 \cap V_n$ for which $\mathbb{Q}_p(\zeta_n)^2 \cap V_n = \mathbb{Q}_p(\zeta_n)\, b$. But then $\mathbb{Q}_p(\zeta_n)^2 \cap V_n$ is an irreducible faithful $\mathbb{Q}_p[\mu_{p^n}]$-module on which τ_n acts trivially, which contradicts the fact that the only irreducible representation of D_n having τ_n in its kernel is the trivial one.

All that remains is to prove that if $B' = \{b_0', b_1'\}$ is a $\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]$-basis for $V_p(J_n^-)$ then it is a $\mathbb{Q}_p[\mu_{p^n}]$-basis for $V_p(J_n)$. Let $B = \{b_0, b_1\} \subset V_p(J_n^-)$ be a $\mathbb{Q}_p[\mu_{p^n}]$-basis for $V_p(J_n)$. From above, B is also a $\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]$-basis for $V_p(J_n^-)$, and therefore writing $b_0' = \alpha_{0,0} b_0 + \alpha_{1,0} b_1, b_1' = \alpha_{0,1} b_0 + \alpha_{1,1} b_1$ with

$\alpha_{i,j} \in \mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]$, the matrix $M = (\alpha_{i,j})_{0 \le i,j \le 1}$ is invertible. Extending scalars to $\mathbb{Q}_p[\mu_{p^n}]$, M remains invertible, so B' is indeed a $\mathbb{Q}_p[\mu_{p^n}]$-basis for $V_p(J_n)$. $\square$

Since the action of $G_{\mathbb{Q}(\mu_{p^\infty},t)}$ on $V_p(J_n)$ and $V_p(J_n^-)$ commutes with the actions of $\mathbb{Q}_p[\mu_{p^n}]$ and $\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]$ respectively, choosing a $\mathbb{Q}_p[\mu_{p^n}]$-basis B for $V_p(J_n)$ contained in $V_p(J_n^-)$, the action of $G_{\mathbb{Q}(\mu_{p^\infty},t)}$ on $V_p(J_n)$ and $V_p(J_n^-)$ respectively gives representations

$$\begin{aligned} \rho_n : G_{\mathbb{Q}(\mu_{p^\infty},t)} &\longrightarrow \mathrm{GL}_2\left(\mathbb{Q}_p[\mu_{p^n}]\right) \\ \text{and} \qquad \rho_n^- : G_{\mathbb{Q}(\mu_{p^\infty},t)} &\longrightarrow \mathrm{GL}_2\left(\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]\right). \end{aligned}$$

Since the basis is the same for both representations, ρ_n is simply the representation obtained from ρ_n^- by extending scalars to $\mathbb{Q}_p[\mu_{p^n}]$. Since the action of $G_{\mathbb{Q}(\mu_{p^\infty},t)}$ commutes with $\phi_{n,m}$, the representations ρ_n are compatible with respect to the maps $\mathbb{Q}_p[\mu_{p^n}] \longrightarrow \mathbb{Q}_p[\mu_{p^m}]$ taking γ_n to γ_m for each $m \le n$. We will show that, with respect to an appropriate basis, the image of ρ_n is contained in $\mathrm{GL}_2(\mathbb{Z}_p[\mu_{p^n}])$, and thus we obtain a representation $\rho^{\mathrm{hg}} : G_{\mathbb{Q}(\mu_{p^\infty},t)} \longrightarrow \mathrm{GL}_2\left(\varprojlim \mathbb{Z}_p[\mu_{p^n}]\right) \cong \mathrm{GL}_2(\mathbb{Z}_p[[T]])$.

4.6 The Reduction Type of C_n, C_n^- and the Associated Galois Representation

In order to understand the local behaviour of the Galois representation

$$\rho_n : G_{\mathbb{Q}(\mu_{p^\infty},t)} \longrightarrow \mathrm{GL}_2\left(\mathbb{Q}_p[\mu_{p^n}]\right),$$

we will consider the reduction type of C_n and C_n^- at various places. By the above discussion, ρ_n may be viewed as the representation associated to C_n^- by composing with the natural inclusion $\mathrm{GL}_2\left(\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]\right) \hookrightarrow \mathrm{GL}_2\left(\mathbb{Q}_p[\mu_{p^n}]\right)$, so we will no longer distinguish between the two representations. Thus we may obtain information about ρ_n by considering either C_n or C_n^-.

Proposition 4.22 *As a curve over $\overline{\mathbb{Q}}(t)$, C_n has good reduction outside $t = 0, 1, \infty$.*

Proof: For $t \in \overline{\mathbb{Q}}$, the curve $C_n(t)/\overline{\mathbb{Q}}$ given by

$$C_n(t) : y^2 = f(x) = x\left(x^{2p^n} + (4t-2)x^{p^n} + 1\right)$$

is singular if and only if $f(x)$ has a repeated root. The roots of $f(x)$ are given by

$$x = 0,\ \zeta_n^j\left(\frac{-(4t-2) \pm \sqrt{(4t-2)^2 - 4}}{2}\right) \qquad j = 0, \dots, p^n - 1.$$

Thus $f(x)$ has a repeated root if and only if

$$-(4t-2) + \sqrt{(4t-2)^2 - 4} = \zeta_n^j\left(-(4t-2) - \sqrt{(4t-2)^2 - 4}\right)$$

for some j. Solving gives $t = 0$ or 1.

Whenever $t \neq 0, 1, \infty$, one may apply the argument of the proof of Proposition 4.16 to show that the genus of $C_n(t)$ is the same as that of C_n. $\square$

Corollary 4.23 *The representation ρ_n factors through $\Pi_{\mathbb{Q}(\mu_{p^\infty}, t)}$.*

Proof: By Proposition 4.8, $\rho_n^{\mathrm{geom}} = \rho_n|_{\Pi_{\overline{\mathbb{Q}}}}$ is unramified outside $t = 0, 1, \infty$, and hence factors through the Galois group of the maximal algebraic extension $\widehat{\overline{\mathbb{Q}}(t)}$ of $\overline{\mathbb{Q}}(t)$ unramified outside $t = 0, 1, \infty$. The result now follows from Corollary 3.4 with $K = \mathbb{Q}(\mu_{p^\infty})$. $\square$

The residual representation $\bar{\rho}$ of each ρ_n is the representation of $\Pi_{\mathbb{Q}(\mu_{p^\infty})}$ describing the action on the p-torsion points of the elliptic curve C_0. Let $E_L/\mathbb{Q}(t)$ denote the Legendre family of elliptic curves

$$E_L : y^2 = x(x-1)(x-t).$$

There is a 2-isogeny $\phi : C_0 \longrightarrow E_L$ given by

$$\phi : (x, y) \longmapsto \left(-\frac{y^2}{4x^2} + t, \frac{iy(1-x^2)}{8x^2} \right);$$

in particular, $\bar{\rho}^{\mathrm{geom}} = \bar{\rho}|_{\Pi_{\overline{\mathbb{Q}}}}$ is also the representation of $\Pi_{\overline{\mathbb{Q}}}$ attached to the p-torsion points of E_L. In order to determine $\bar{\rho}^{\mathrm{geom}}$ explicitly, we first need a lemma:

Lemma 4.24 *Let $E_1 : y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve defined over a field K, and let $\rho_1 : G_K \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$ be the Galois representation associated to E_1. For any $d \in K^\times$, the twist*

$$E_2 : dy^2 = x^3 + ax^2 + bx + c$$

of E_1 has the associated Galois representation $\rho_2 = \rho_1 \otimes \chi_{K(\sqrt{d})/K}$, where

$$\chi_{K(\sqrt{d})/K}(\sigma) = \begin{cases} 1 & \textit{if } \sigma \textit{ fixes } \sqrt{d}, \\ -1 & \textit{otherwise.} \end{cases}$$

Proof: Fix an $\mathbb{F}_p$-basis $\{(x_0, y_0), (x_1, y_1)\}$ for the p-torsion points of E_1. The map $\phi_{\sqrt{d}} : E_1 \longrightarrow E_2$ defined by $\phi_{\sqrt{d}}(x, y) = \left(x, \frac{y}{\sqrt{d}}\right)$ is an isomorphism of elliptic curves, so $\left\{\left(x_0, \frac{y_0}{\sqrt{d}}\right), \left(x_1, \frac{y_1}{\sqrt{d}}\right)\right\}$ is an $\mathbb{F}_p$-basis for the p-torsion points of E_2; moreover, if $\sigma \cdot (x_i, y_i) = a_0(x_0, y_0) + a_1(x_1, y_1)$, then for $\sigma \in G_K$,

$$\sigma \cdot \left(x_i, \tfrac{y_i}{\sqrt{d}}\right) = a_0 \left(x_0, \tfrac{y_0}{\sigma(\sqrt{d})}\right) + a_1 \left(x_1, \tfrac{y_1}{\sigma(\sqrt{d})}\right).$$

If $\sigma(\sqrt{d}) = \sqrt{d}$, then $\sigma \cdot \left(x_i, \frac{y_i}{\sqrt{d}}\right) = a_0 \left(x_0, \frac{y_0}{\sqrt{d}}\right) + a_1 \left(x_1, \frac{y_1}{\sqrt{d}}\right)$ for $i = 0, 1$. Otherwise, $\sigma(\sqrt{d}) = -\sqrt{d}$, and thus

$$\begin{aligned} \sigma \cdot \left(x_i, \tfrac{y_i}{\sqrt{d}}\right) &= a_0 \left(x_0, -\tfrac{y_0}{\sqrt{d}}\right) + a_1 \left(x_1, -\tfrac{y_1}{\sqrt{d}}\right) \\ &= -a_0 \left(x_0, \tfrac{y_0}{\sqrt{d}}\right) - a_1 \left(x_1, \tfrac{y_1}{\sqrt{d}}\right), \end{aligned}$$

as desired. $\square$

Proposition 4.25 *The representation $\bar{\rho}^{\text{geom}}$ satisfies*

$$\bar{\rho}^{\text{geom}}(\sigma_0) \sim \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \textit{and} \quad \bar{\rho}^{\text{geom}}(\sigma_1) \sim \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix}.$$

Proof: At $t = 0$, C_0 reduces to the curve

$$C_0(0) : y^2 = x(x-1)^2,$$

whose only singularity is a node at the point $(1,0)$. Let N_0 be the genus 0 curve defined by $N_0 : y^2 = x$. There is a birational map $\phi_0 : C_0(0) \longrightarrow N_0$ given by

$$\phi_0 : (x,y) \longrightarrow \left(x, \frac{y}{x-1}\right),$$

so $C_0(0)$ is birationally equivalent to a projective line. Therefore, C_0 is a Mumford curve at $t = 0$, and Corollary 4.12 gives $\bar{\rho}^{\text{geom}}(\sigma_0) \sim \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. A similar argument shows that $\bar{\rho}^{\text{geom}}(\sigma_1) \sim \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ as well.

For the reduction at $t = \infty$, consider the twist C_0' of C_0 given by

$$C_0' : ty^2 = x^3 + (4t-2)x^2 + x.$$

Letting $u = \frac{1}{t}$ and replacing x with $\frac{u}{x}$ and y with $\frac{uy}{x^2}$ gives the model

$$y^2 = x^3 + (4-2u)x^2 + u^2 x$$

for C_0'. At $u = 0$ (that is, at $t = \infty$), this model reduces to

$$y^2 = x^2(x+4),$$

which is a projective line with a nodal singularity at the point $(0,0)$; therefore, C_0' is a Mumford curve at $t = \infty$. Since $\sigma_\infty(\sqrt{t}) = -\sqrt{t}$, Lemma 4.24 gives $\bar{\rho}^{\text{geom}}(\sigma_\infty) \sim \left(\begin{smallmatrix} -1 & -1 \\ 0 & -1 \end{smallmatrix}\right)$.

Fixing an $\mathbb{F}_p$-basis for the p-torsion points of C_0 with respect to which $\bar{\rho}^{\text{geom}}(\sigma_0) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, we cannot have $\bar{\rho}^{\text{geom}}(\sigma_1) = \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ since $\bar{\rho}^{\text{geom}}(\sigma_\infty)$ has order $2p$. Thus changing basis if necessary, we may assume that $\bar{\rho}^{\text{geom}}(\sigma_1) = \left(\begin{smallmatrix} 1 & 0 \\ \alpha & 1 \end{smallmatrix}\right)$

for some $\alpha \in \mathbb{F}_p^\times$. Multiplying gives

$$\bar{\rho}^{\text{geom}}(\sigma_\infty) = (\bar{\rho}^{\text{geom}}(\sigma_0)\bar{\rho}^{\text{geom}}(\sigma_1))^{-1} = \begin{pmatrix} 1 & -1 \\ -\alpha & 1+\alpha \end{pmatrix};$$

in particular, $\operatorname{tr} \bar{\rho}^{\text{geom}}(\sigma_\infty) = 2 + \alpha$. On the other hand, $\operatorname{tr} \bar{\rho}^{\text{geom}}(\sigma_\infty) = -2$ since $\bar{\rho}^{\text{geom}}(\sigma_\infty) \sim \left(\begin{smallmatrix} -1 & -1 \\ 0 & -1 \end{smallmatrix}\right)$, and thus $\alpha = -4$. $\square$

To examine the reduction type of C_n^- at $t = 0, 1$, we will use some identities which appear in [Dar00], p.420.

Lemma 4.26 *Let $g_n(x)$ be as in Proposition 4.13. Then*

$$xg_n(x^2 - 2) = g_n(-x)^2(x - 2) + 2 = g_n(x)^2(x + 2) - 2.$$

Proof: First we will show that $xg_n(x^2-2)-2 = g_n(-x)^2(x-2)$. From (4.14), we have

$$x^{p^n} + x^{-p^n} = (x + x^{-1})g_n(x^2 + x^{-2}). \tag{4.27}$$

Thus putting $x = \zeta_n^j + \zeta_n^{-j}$ into $xg(x^2 - 2) - 2$ gives

$$(\zeta_n^j + \zeta_n^{-j})g_n(\zeta_n^{2j} + \zeta_n^{-2j}) - 2 = (\zeta_n^j)^{p^n} + (\zeta_n^j)^{-p^n} - 2 = 0,$$

so $\zeta_n^j + \zeta_n^{-j}$ is a root of $xg_n(x^2 - 2) - 2$ for each $j = 0, \ldots, \frac{p^n-1}{2}$. Since $g_n(x) = \prod_{j=1}^{\frac{p^n-1}{2}} (x + \zeta_n^j + \zeta_n^{-j})$, each $\zeta_n^j + \zeta_n^{-j}$ is also a root of $g_n(-x)^2(x - 2)$.

Taking $x = -\zeta_n^j - \zeta_n^{-j}$ gives

$$-(\zeta_n^j + \zeta_n^{-j}) g_n(\zeta_n^{2j} + \zeta_n^{-2j}) - 2 = -4,$$

and replacing j with $j + p^n$ if necessary so that j is even,

$$\begin{aligned} g_n(\zeta_n^j + \zeta_n^{-j})^2(-\zeta_n^j - \zeta_n^{-j} - 2) &= g_n\left((\zeta_n^{j/2})^2 + (\zeta_n^{j/2})^{-2}\right)^2 (-\zeta_n^j - \zeta_n^{-j} - 2) \\ &= \left(\frac{(\zeta_n^{j/2})^{p^n} + (\zeta_n^{j/2})^{-p^n}}{\zeta_n^{j/2} + \zeta_n^{-j/2}}\right)^2 (-\zeta_n^j - \zeta_n^{-j} - 2) \\ &= \frac{4}{\zeta_n^j + \zeta_n^{-j} + 2}(-\zeta_n^j - \zeta_n^{-j} - 2) = -4, \end{aligned}$$

so $xg_n(x^2-2)-2$ and $g_n(-x)^2(x-2)$ also agree at the $\frac{p^n+1}{2}$ points $-\zeta_n^j - \zeta_n^{-j}$ for $j = 0, \ldots, \frac{p^n-1}{2}$. Thus $xg_n(x^2-2)-2$ and $g_n(-x)^2(x-2)$ are polynomials of degree p^n which agree at p^n+1 points, and hence are equal.

Since $xg_n(x^2-2)$ is odd,

$$\begin{aligned} xg_n(x^2-2) &= -(-x)g_n((-x)^2-2) \\ &= -\left(g_n\left(-(-x)\right)^2(-x-2)+2\right) \\ &= g_n(x)^2(x+2)-2, \end{aligned}$$

as desired. $\square$

Proposition 4.28 *The curve C_n^- is a Mumford curve at $t=0$ and $t=1$.*

Proof: Using the identity $xg_n(x^2-2) = g_n(-x)^2(x-2)+2$, we have

$$C_n^- : y^2 = g_n(-x)^2(x-2) + 4t.$$

At $t = 0$, this reduces to the curve $C_n^-(0) : y^2 = g_n(-x)^2(x-2)$, whose singularities consist of ordinary double points at $(\zeta_n^j + \zeta_n^{-j}, 0)$ for each $j = 1, \dots, \frac{p^n-1}{2}$. The map from $C_n^-(0)$ to $N : y^2 = x - 2$ which takes (x, y) to $\left(x, \frac{y}{g(-x)}\right)$ defines a birational equivalence between $C_n^-(0)$ and a curve of genus zero, that is, a projective line.

The argument for $t = 1$ is similar, except that one uses instead the identity $xg_n(x^2 - 2) = g_n(x)^2(x + 2) - 2$. $\square$

To calculate the image of the inertia group at $t = \infty$, we view C_n^- as being defined over the field $\overline{\mathbb{Q}}\left(\left(\frac{1}{t}\right)\right)$.

Proposition 4.29 *The curve C_n^- acquires good reduction at $t = \infty$ over the field $\overline{\mathbb{Q}}\left(\left(\left(\frac{1}{t}\right)^{1/2p^n}\right)\right)$.*

Proof: Let $u = \left(\frac{1}{t}\right)^{1/2p^n}$. Consider the curve $\tilde{C}_n^-/\overline{\mathbb{Q}}((u))$ given by

$$\tilde{C}_n^- : y^2 = x \prod_{j=1}^{\frac{p^n-1}{2}} \left(1 + (\zeta_n^j + \zeta_n^{-j} - 2)u^4x^2\right) + (4 - 2u^{2p^n})x^{p^n+1}.$$

There is an isomorphism $\phi : \tilde{C}_n^- \longrightarrow C_n^-$ defined over $\overline{\mathbb{Q}}((u))$ given by

$$\phi : (x, y) \longmapsto \left(\frac{1}{u^2x}, \frac{y}{u^{p^n}x^{\frac{p^n+1}{2}}}\right).$$

Reducing $\tilde{C}_n^-$ at $u = 0$ (that is, at $t = \infty$) gives the nonsingular curve

$$\tilde{C}_n^-(\infty) : y^2 = 4x^{p^n+1} + x,$$

which has genus $\frac{p^n-1}{2}$. $\square$

Corollary 4.30 *The inertia group $I_\infty \subset \Pi_{\overline{\mathbb{Q}}}$ at $t = \infty$ is mapped by ρ_n to a subgroup of* $\mathrm{GL}_2(\mathbb{Q}_p[\mu_{p^n}])$ *of order dividing $2p^n$.*

Proof: By Proposition 4.8, the restriction of ρ_n to I_∞ factors through the Galois group $\mathrm{Gal}\left(\overline{\mathbb{Q}}\left(\left(\left(\frac{1}{t}\right)^{1/2p^n}\right)\right) / \overline{\mathbb{Q}}\left(\left(\frac{1}{t}\right)\right)\right)$, which has order $2p^n$. $\square$

We were not able to give an elementary proof that $\rho_n(I_\infty)$ has order exactly $2p^n$, because of the difficulty in understanding in general when a curve with bad reduction at a particular place may have a Jacobian with good reduction at that place. This result will follow, however, from a general construction of Katz.

4.7 A Theorem of Katz

Let $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{Q}$ be such that $\alpha_i - \beta_j$ is not an integer for any $i, j = 1, 2$. Suppose that

$$\kappa : \Pi_{\overline{\mathbb{Q}}} \longrightarrow \mathrm{GL}_2(\mathbb{Q}_p(\zeta_n))$$

is such that $\kappa(\sigma_0)$ has eigenvalues $e^{2\pi i\alpha_1}, e^{2\pi i\alpha_2}$, $\kappa(\sigma_1)$ has repeated eigenvalue 1, and $\kappa(\sigma_\infty)$ has eigenvalues $e^{2\pi i\beta_1}, e^{2\pi i\beta_2}$. According to a theorem of Belyĭ, such a representation is unique up to conjugation by an element of $\mathrm{GL}_n(\mathbb{Q}_p(\zeta_n))$. To be precise, Belyĭ's theorem asserts that for any field k, if $M_0, M_1 \in \mathrm{GL}_n(k)$ generate an irreducible subgroup of $\mathrm{GL}_n(k)$, and one of M_0, M_1, or $(M_0M_1)^{-1}$ differs from a scalar matrix by a matrix of rank one, then $(M_0, M_1, (M_0M_1)^{-1})$ is rigid in $\mathrm{GL}_n(k)$ (see [Bel80], Theorem 2).

Note that if $A/\overline{\mathbb{Q}}(t)$ is an abelian variety of dimension $p^n - p^{n-1}$ which contains $\mathbb{Z}[\zeta_n]$ in its endomorphism ring, then $V_p(A)$ is a vector space of dimension 2 over $\mathbb{Q}_p(\zeta_n)$; if, moreover, A has good reduction outside $t = 0, 1, \infty$, then the action of $\Pi_{\overline{\mathbb{Q}}}$ on $V_p(A)$ gives rise to a 2-dimensional representation of $\Pi_{\overline{\mathbb{Q}}}$ over $\mathbb{Q}_p(\zeta_n)$. Katz' theorem realizes κ as the representation associated to such an abelian variety A defined over $\mathbb{Q}(t)$.

Let N be a common denominator for $\alpha_1, \alpha_2, \beta_1, \beta_2$, and let $A(j) = N\alpha_j$, $B(j) = N\beta_j \in \mathbb{Z}$ for each $j = 1, 2$. The nonsingular curve $\tilde{D}/\mathbb{Q}(t)$ defined by

$$\tilde{D} : \begin{cases} x_1^N = y_1^{A(1)}(1 - y_1)^{B(1)-A(1)} \\ x_2^N = y_2^{A(2)}(1 - y_2)^{B(2)-A(2)} \\ y_1 y_2 = t \end{cases}$$

possesses a natural action of $\mu_N \times \mu_N \subset \bar{\mathbb{Q}} \times \bar{\mathbb{Q}}$ by

$$(\zeta_N^j, \zeta_N^l) \cdot (x_1, y_1, x_2, y_2) = (\zeta_N^j x_1, y_1, \zeta_N^l x_2, y_2)$$

for each $j, l \in \mathbb{Z}/p^n\mathbb{Z}$, $(x_1, y_1, x_2, y_2) \in \tilde{D}(\overline{\mathbb{Q}(t)})$, where ζ_N is a primitive Nth root of unity. Defining a character

$$\begin{aligned} \chi : \mu_N \times \mu_N &\longrightarrow \overline{\mathbb{Q}}^{\times} \\ (\zeta_N^j, \zeta_N^l) &\longmapsto \zeta_N^{j+l}, \end{aligned}$$

$\ker(\chi)$ is the subgroup of $\mu_N \times \mu_N$ consisting of elements of the form $(\zeta_N^j, \zeta_N^{-j})$. Let D be the quotient of $\tilde{D}$ by the group of automorphisms $\ker(\chi)$.

Theorem 4.31 *The Jacobian of D has a quotient A of dimension $p^n - p^{n-1}$ whose endomorphism ring contains $\mathbb{Z}[\zeta_n]$, and whose associated representa-*

tion of $\Pi_{\overline{\mathbb{Q}}}$ *is* κ.

Proof: See [Kat90], Theorem 5.4.4. $\square$

Remark: Theorem 5.4.4 of [Kat90] more generally gives geometric constructions of n-dimensional representations

$$\kappa : \Pi_{\overline{\mathbb{Q}}} \longrightarrow \mathrm{GL}_n\left(\mathbb{Q}_p(\zeta_n)\right)$$

for any choice of eigenvalues $e^{2\pi i\alpha_1}, \ldots, e^{2\pi i\alpha_n}$ of $\kappa(\sigma_0)$, and $e^{2\pi i\beta_1}, \ldots, e^{2\pi i\beta_n}$ of $\kappa(\sigma_\infty)$, where $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbb{Q}$ satisfy the condition that $\alpha_i - \beta_j$ is not an integer for any i, j; again $\kappa(\sigma_1)$ has repeated eigenvalue 1.

In order to show that $\rho_n(\sigma_\infty)$ has order $2p^n$, we use Theorem 4.31 with $\alpha_1 = \alpha_2 = 0$, $\beta_1 = \frac{1}{2p^n}$, and $\beta_2 = -\frac{1}{2p^n}$; thus we will construct a representation

$$\kappa_n : \Pi_{\overline{\mathbb{Q}}} \longrightarrow \mathrm{GL}_2\left(\mathbb{Q}_p(\zeta_n)\right)$$

such that $\kappa_n(\sigma_0)$, $\kappa_n(\sigma_1)$ each have repeated eigenvalue 1, and $\kappa_n(\sigma_\infty)$ has eigenvalues $-\zeta_n$, $-\zeta_n^{-1}$, where ζ_n is a primitive p^nth root of unity. Taking $N = 2p^n$, we obtain $A(1) = A(2) = 0$, $B(1) = 1$, and $B(2) = -1$. Let $\tilde{D}_n/\overline{\mathbb{Q}}(t)$ be the curve defined by

$$\tilde{D}_n : \begin{cases} X_1^{2p^n} = 1 - Y_1 \\ X_2^{2p^n} = (1 - Y_2)^{-1} \\ Y_1 Y_2 = t. \end{cases} \tag{4.32}$$

With χ as above, let D_n denote the quotient curve $\tilde{D}_n/\ker(\chi)$. The subfield of the function field of $\tilde{D}_n$ consisting of those elements invariant under $\ker(\chi)$

is generated over $\overline{\mathbb{Q}(t)}$ by

$$y = Y_1 = t/Y_2 \quad \text{and} \quad x = X_1 X_2.$$

From (4.32), we see that a model for D_n is given by

$$D_n : x^{2p^n} = (1-y)\left(1 - \frac{t}{y}\right)^{-1}.$$

For each n, let D_n° be the curve defined by

$$D_n^\circ : x^{p^n} = (1-y)\left(1 - \frac{t}{y}\right)^{-1}.$$

Let K_n and K_n° denote the Jacobians of D_n and D_n° respectively. Let $\pi_n : D_n \longrightarrow D_{n-1}$ be the morphism mapping (x, y) to (x^p, y), and let $\pi_n^\circ : D_n \longrightarrow D_n^\circ$ be the morphism mapping (x, y) to (x^2, y).

There is a natural action of μ_{p^n} on D_n and on D_n° by $\gamma_n(x, y) = (\zeta_n x, y)$, which satisfies the relations

$$\pi_n \circ \gamma_n = \gamma_{n-1} \circ \pi_n \quad \text{and} \quad \pi_n^\circ \circ \gamma_n = \gamma_n^2 \circ \pi_n^\circ,$$

provided that the generators γ_n of each μ_{p^n} are chosen so that $\zeta_n^p = \zeta_{n-1}$. Thus $V_p(K_n)$, $V_p(K_n^\circ)$, and $V_p(K_{n-1})$ are $\mathbb{Q}_p[\mu_{p^n}]$-modules, and the morphisms π_n, π_n° induce $\mathbb{Q}_p[\mu_{p^n}]$-module inclusions

$$\pi_n^* : V_p(K_{n-1}) \hookrightarrow V_p(K_n) \quad \text{and} \quad (\pi_n^\circ)^* : V_p(K_n^\circ) \hookrightarrow V_p(K_n).$$

On the other hand, D_n is related to C_n by the morphism

$$\begin{aligned} \psi_n : D_n &\longrightarrow C_n \\ (x,y) &\longmapsto \left(x^2,\ x^{p^n+1}\left(\frac{2(y+ty^{-1}-1)+x^{2p^n}+x^{-2p^n}}{x^{p^n}+x^{-p^n}}\right)\right). \end{aligned}$$

We define abelian varieties

$$\begin{aligned} A_n &:= K_n / \left(\pi_n^*(K_{n-1}) + (\pi_n^\circ)^*(K_n^\circ)\right), \\ J_n^{\mathrm{new}} &:= J_n / \phi_{n,n-1}^*(J_{n-1}). \end{aligned}$$

Let $p_n : K_n \longrightarrow A_n$ be the natural projection.

Proposition 4.33 *The abelian variety A_n is the quotient of K_n of Theorem* 4.31, *and the map $p_n \circ \psi_n^* : J_n \longrightarrow A_n$ induces a $\mathbb{Q}_p(\zeta_n)$-vector space isomorphism $V_p(J_n^{\mathrm{new}}) \cong V_p(A_n)$ which commutes with the action of $\Pi_{\overline{\mathbb{Q}}}$. In particular, the eigenvalues of σ_∞ as a $\mathbb{Q}_p(\zeta_n)$-linear map on $V_p(J_n^{\mathrm{new}})$ are $-\zeta_n, -\zeta_n^{-1}$.*

Proof: A computation using the Riemann-Hurwitz formula shows that the genus of D_n is $2p^n - 1$, and that of D_n° is $p^n - 1$. If we show that

$$(\pi_n^\circ)^*\left(V_p(K_n^\circ)\right) \bigcap \psi_n^*\left(V_p(J_n)\right) = \{0\},$$

then counting $\mathbb{Q}_p$-dimensions, we must have

$$V_p(K_n) \cong V_p(K_n^\circ) \oplus V_p(J_n). \tag{4.34}$$

Let σ be the involution of D_n which maps (x,y) to $(-x,y)$, so that

$D_n^\circ = D_n/\langle\sigma\rangle$. Then $\sigma_* : K_n \longrightarrow K_n$ fixes each point in $(\pi_n^\circ)^*(K_n^\circ)$. On the other hand, letting h denote the hyperelliptic involution $h : (x, y) \longmapsto (x, -y)$ on C_n, we have the relation $\psi_n \circ \sigma = h \circ \psi_n$. Since h_* acts as -1 on J_n, σ_* acts as -1 on $\psi_n^*(J_n)$; in particular, σ_* acts nontrivially on every element of $\psi_n^*(J_n)$ which does not have order 2. Therefore, $(\pi_n^\circ)^*(K_n^\circ) \cap \psi_n^*(J_n)$ is contained in $K_n[2]$, and in particular $(\pi_n^\circ)^*(V_p(K_n^\circ)) \cap \psi_n^*(V_p(J_n)) = \{0\}$, as desired.

A similar analysis to that in the proof of Proposition 4.19 shows that there is a $\mathbb{Q}_p[\mu_{p^n}]$-module isomorphism

$$V_p(K_n^\circ) \cong \mathbb{Q}_p(\zeta_n)^2 \oplus \cdots \oplus \mathbb{Q}_p(\zeta_1)^2.$$

Thus by (4.34), we have

$$V_p(K_n) \cong \mathbb{Q}_p(\zeta_n)^4 \oplus \cdots \oplus \mathbb{Q}_p(\zeta_1)^4 \oplus \mathbb{Q}_p^2$$

for each $n \geq 1$. Since π_n^* and $(\pi_n^\circ)^*$ are $\mathbb{Q}_p[\mu_{p^n}]$-module inclusions,

$$\begin{aligned}&\pi_n^*(V_p(K_{n-1})) + (\pi_n^\circ)^*(V_p(K_n^\circ))\\ &\qquad\cong \mathbb{Q}_p(\zeta_n)^2 \oplus \mathbb{Q}_p(\zeta_{n-1})^4 \oplus \cdots \oplus \mathbb{Q}_p(\zeta_1)^4 \oplus \mathbb{Q}_p^2,\end{aligned}$$

and therefore $V_p(A_n) \cong \mathbb{Q}_p(\zeta_n)^2$. Let $K_n^{\mathrm{new}} := K_n/\pi_n^*(K_{n-1})$, and let $(K_n^\circ)^{\mathrm{new}} := K_n^\circ/(\pi_{n,n-1}^\circ)^*(K_{n-1}^\circ)$, where $\pi_{n,n-1}^\circ : D_n^\circ \longrightarrow D_{n-1}^\circ$ is given by $\pi_{n,n-1}^\circ(x, y) = (x^p, y)$; thus $V_p(K_n^{\mathrm{new}}) \cong \mathbb{Q}_p(\zeta_n)^4$ and $V_p((K_n^\circ)^{\mathrm{new}}) \cong \mathbb{Q}_p(\zeta_n)^2$. Note that D_n° is the curve constructed by Theorem 4.31 when $\alpha_1 = \alpha_2 = 0$, $\beta_1 = \frac{1}{p^n}$, and $\beta_2 = \frac{-1}{p^n}$. The abelian variety $(K_n^\circ)^{\mathrm{new}}$ is the only quotient of K_n° of dimension $p^n - p^{n-1}$ which contains $\mathbb{Z}[\zeta_n]$ in its endomorphism ring, so by

Theorem 4.31, σ_∞ has eigenvalues ζ_n, ζ_n^{-1} as a $\mathbb{Q}_p(\zeta_n)$-linear automorphism of $V_p\left((K_n^\circ)^{\mathrm{new}}\right)$.

Let $K \subset K_n^{\mathrm{new}}$ be such that K_n^{new}/K is the quotient of Theorem 4.31. Then $V_p(K) \subset V_p(K_n^{\mathrm{new}})$ must contain the eigenvectors of σ_∞ corresponding to the eigenvalues ζ_n, ζ_n^{-1}, for otherwise σ_∞ would have at least three distinct eigenvalues as a $\mathbb{Q}_p(\zeta_n)$-linear automorphism of the 2-dimensional vector space $V_p(K_n^{\mathrm{new}})$. Therefore, $V_p(K) = (\pi_n^\circ)^* \left(V_p(K_n^\circ)\right)$, so A_n is the quotient of Theorem 4.31. Moreover, the inclusion ψ_n^* composed with the natural map $V_p(K_n) \longrightarrow V_p(A_n)$ induces a $\mathbb{Q}_p(\zeta_n)$-vector space isomorphism

$$(\psi_n^*)^{\mathrm{new}} : V_p(J_n^{\mathrm{new}}) \longrightarrow V_p(A_n).$$

Since the isomorphism of (4.34) commutes with the action of $\Pi_{\overline{\mathbb{Q}}}$, so does $(\psi_n^*)^{\mathrm{new}}$. $\square$

Proposition 4.35 *The $\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]$-module $V_n = V_p(J_n^-) \oplus V_p(J_0)$ has a basis $\{b_0, b_1\}$ with respect to which*

$$\rho_n(\sigma_0) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho_n(\sigma_1) = \begin{pmatrix} 1 & 0 \\ \alpha_n & 1 \end{pmatrix}$$

for some $\alpha_n \in \mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]^\times$.

Proof: By Proposition 4.25, the representation $\rho_0^{\mathrm{geom}} = \rho_0|_{\Pi_{\overline{\mathbb{Q}}}}$ is given by

$$\rho_0(\sigma_0) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \rho_0(\sigma_1) = \begin{pmatrix} 1 & 0 \\ \alpha_0 & 1 \end{pmatrix}$$

for some $\alpha_0 \in \mathbb{Z}_p^\times$ reducing to $-4 \mod p$. Thus by Proposition 4.28 and Corollary 4.12, the p-adic representation $\tilde{\rho}_n : \Pi_{\overline{\mathbb{Q}}} \longrightarrow \mathrm{GL}_{p^n+1}(\mathbb{Q}_p)$ satisfies

$$\tilde{\rho}_n(\sigma_i) \sim \left(\begin{array}{cccc|cccc|cc} 1 & 0 & \dots & 0 & * & * & \dots & * & 0 & 0 \\ 0 & 1 & \dots & 0 & * & * & \dots & * & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & * & * & \dots & * & 0 & 0 \\ \hline 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ \hline 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & 1 \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 1 \end{array}\right) \tag{4.36}$$

for each $i = 0, 1$.

We now proceed by induction on n. When $n = 0$, the result follows from above. Assume that there is such a basis for V_{n-1}. Choosing a p^nth root of unity $\zeta_n \in \overline{\mathbb{Q}}_p$ gives rise to an isomorphism

$$\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}] \cong \mathbb{Q}_p(\zeta_n + \zeta_n^{-1}) \oplus \mathbb{Q}_p[\gamma_{n-1} + \gamma_{n-1}^{-1}],$$

and thus also a $\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]$-module isomorphism

$$V_n \cong \mathbb{Q}_p(\zeta_n + \zeta_n^{-1})^2 \oplus V_{n-1}.$$

By assumption, there is a basis $\{b_{0,n-1}, b_{1,n-1}\}$ for V_{n-1} which satisfies

$\sigma_i \cdot b_{i,n-1} = b_{i,n-1}$ for $i = 0, 1$. From (4.36), σ_0 fixes a $\mathbb{Q}_p$-subspace of V_n of dimension $\frac{p^n+1}{2}$, and since there is a nontrivial subspace of $V_p(J_0)$ not fixed by σ_0, σ_0 fixes a subspace of V_{n-1} of dimension at most p^{n-1}. Since $p > 2 > 2 - \frac{1}{p^{n-1}}$, we have $\frac{p^n+1}{2} > p^{n-1}$, so there some nonzero element $\hat{b}_0 \in \mathbb{Q}_p(\zeta_n + \zeta_n^{-1})^2$ fixed by σ_0. Let $b_0 = \hat{b}_0 + b_{0,n-1}$. Since $b_{0,n-1}$ generates a free module over $\mathbb{Q}_p[\gamma_{n-1} + \gamma_{n-1}^{-1}]$ and $\mathbb{Q}_p(\zeta_n + \zeta_n^{-1})$ is a field, b_0 generates a free module over $\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]$. By the same argument, there is an element $b_1 \in V_n$ fixed by σ_1 which generates a free module over $\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]$.

We claim that $\{b_0, b_1\}$ is a $\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]$-basis for V_n. Let $\hat{b}_1 = b_1 - b_{1,n-1}$, so $\hat{b}_1 \in \mathbb{Q}_p(\zeta_n + \zeta_n^{-1})^2$. It suffices to show that σ_0 and σ_1 have no common nontrivial fixed point in $\mathbb{Q}_p(\zeta_n + \zeta_n^{-1})^2$, for then in particular we have

$$\mathbb{Q}_p(\zeta_n + \zeta_n^{-1})\, \hat{b}_0 \bigcap \mathbb{Q}_p(\zeta_n + \zeta_n^{-1})\, \hat{b}_1 = \{0\}.$$

Let

$$\hat{\rho}_n : \Pi_{\overline{\mathbb{Q}}} \longrightarrow \mathrm{GL}_2\left(\mathbb{Q}_p(\zeta_n + \zeta_n^{-1})\right)$$

be the representation obtained by composing ρ_n with the natural projection $\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}] \longrightarrow \mathbb{Q}_p(\zeta_n + \zeta_n^{-1})$. Let W be a subspace of $\mathbb{Q}_p(\zeta_n + \zeta_n^{-1})^2$ satisfying $\mathbb{Q}_p(\zeta_n + \zeta_n^{-1})^2 = \mathbb{Q}_p(\zeta_n + \zeta_n^{-1})\, \hat{b}_0 \oplus W$. Given any nonzero $w \in W$, $\{\hat{b}_0, w\}$ is a basis for $\mathbb{Q}_p(\zeta_n + \zeta_n^{-1})^2$, and from (4.36), $\sigma_0 \cdot w = w + w_0$, where $w_0 \in \mathbb{Q}_p(\zeta_n + \zeta_n^{-1})^2$ is fixed by σ_0. If $\hat{\rho}_n(\sigma_0)$ is nontrivial, then $\mathbb{Q}_p(\zeta_n + \zeta_n^{-1})\, \hat{b}_0$ is the subspace of all σ_0-fixed points, so $w_0 = \beta_0 \hat{b}_0$ for some $\beta_0 \in \mathbb{Q}_p(\zeta_n + \zeta_n^{-1})$, and therefore $\hat{\rho}_n(\sigma_0) = \left(\begin{smallmatrix} 1 & \beta_0 \\ 0 & 1 \end{smallmatrix}\right)$ with respect to the basis $\{\hat{b}_0, w\}$. Similarly, $\hat{\rho}_n(\sigma_1) \sim \left(\begin{smallmatrix} 1 & \beta_1 \\ 0 & 1 \end{smallmatrix}\right)$ for some $\beta_1 \in \mathbb{Q}_p(\zeta_n + \zeta_n^{-1})$. If σ_0, σ_1 have a common fixed point in $\mathbb{Q}_p(\zeta_n+\zeta_n^{-1})^2$, then with respect to some basis we have

$$\hat{\rho}_n(\sigma_0)=\begin{pmatrix}1 & \beta_0\\ 0 & 1\end{pmatrix},\quad \hat{\rho}_n(\sigma_1)=\begin{pmatrix}1 & \beta_1\\ 0 & 1\end{pmatrix}$$

for some $\beta_0,\beta_1\in\mathbb{Q}_p(\zeta_n+\zeta_n^{-1})^2$. Then $\hat{\rho}_n(\sigma_\infty)=\left(\begin{smallmatrix}1 & -(\beta_0+\beta_1)\\ 0 & 1\end{smallmatrix}\right)$, contradicting that $\hat{\rho}_n(\sigma_\infty)$ has exact order $2p^n$. Therefore, σ_0 and σ_1 have no common nontrivial fixed point in $\mathbb{Q}_p(\zeta_n+\zeta_n^{-1})^2$, and $\{b_0,b_1\}$ is indeed a basis for V_n.

By induction, we have

$$\rho_n(\sigma_0)=\begin{pmatrix}1 & \delta_0\\ 0 & 1\end{pmatrix},\quad \rho_n(\sigma_1)=\begin{pmatrix}1 & 0\\ \delta_1 & 1\end{pmatrix}$$

for some $\delta_0,\delta_1\in\mathbb{Q}_p[\gamma_n+\gamma_n^{-1}]$. All that remains is to show that δ_0 and δ_1 are units. Suppose that $\delta_0\notin\mathbb{Q}_p[\gamma_n+\gamma_n^{-1}]^\times$. Writing $\delta_0=\delta_{0,n}+\delta_{0,n-1}$ where $\delta_{0,n}\in\mathbb{Q}_p(\zeta_n+\zeta_n^{-1})$ and $\delta_{0,n-1}\in\mathbb{Q}_p[\gamma_{n-1}+\gamma_{n-1}^{-1}]$, it follows from the inductive hypothesis that $\delta_{0,n-1}\in\mathbb{Q}_p[\gamma_{n-1}+\gamma_{n-1}^{-1}]^\times$, so $\delta_{0,n}$ must not be a unit of $\mathbb{Q}_p(\zeta_n+\zeta_n^{-1})$. Hence $\delta_{0,n}=0$, contradicting that σ_0 acts nontrivially on $\mathbb{Q}_p(\zeta_n+\zeta_n^{-1})^2$. Therefore, $\delta_0\in\mathbb{Q}_p[\gamma_n+\gamma_n^{-1}]^\times$. The same argument shows that $\delta_1\in\mathbb{Q}_p[\gamma_n+\gamma_n^{-1}]^\times$ as well. $\square$

4.8 The Universal Deformation

We now consider the representation obtained by taking the inverse limit of the various representations ρ_n.

Proposition 4.37 *There is a $\mathbb{Q}_p[\mu_{p^n}]$-basis for $V_p(J_n)$ with respect to which* $\mathrm{Im}\rho_n\subset\mathrm{GL}_2(\mathbb{Z}_p[\mu_{p^n}])$.

Proof: By Proposition 4.35, there is a $\mathbb{Q}_p[\mu_{p^n}]$-basis $\mathcal{B}$ for $V_p(J_n)$ with respect to which

$$\rho_n(\sigma_0) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \rho_n(\sigma_1) = \begin{pmatrix} 1 & 0 \\ \alpha_n & 1 \end{pmatrix}.$$

Multiplying gives

$$\rho_n(\sigma_\infty) = \begin{pmatrix} 1 & -1 \\ -\alpha_n & 1+\alpha_n \end{pmatrix}.$$

Since $-\gamma_n$ is an eigenvalue of $\rho_n(\sigma_\infty)$ and ρ_n has determinant one, we have

$$\operatorname{tr} \rho_n(\sigma_\infty) = 2 + \alpha_n = -\gamma_n - \gamma_n^{-1},$$

so $\alpha_n = -(\gamma_n + \gamma_n^{-1} + 2) \in \mathbb{Z}_p[\mu_{p^n}]$. □

To obtain a representation $\rho : \Pi_{\mathbb{Q}(\mu_{p^\infty})} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_p[[T]])$, we need the following result from Iwasawa theory:

Proposition 4.38 *For each compatible system $(\gamma_n)_{n\in\mathbb{N}}$ of generators γ_n of μ_{p^n}, the map sending $(\gamma_n)_{n\in\mathbb{N}}$ to $1+T$ defines an isomorphism*

$$\varprojlim \mathbb{Z}_p[\mu_{p^n}] \cong \mathbb{Z}_p[[T]].$$

Proof: See [Was82], Theorem 7.1. □

For each n, let γ_n be a generator of μ_{p^n} such that $-\gamma_n$ is an eigenvalue of $\rho_n(\sigma_\infty)$. The compatible system $(\gamma_n)_{n\in\mathbb{N}}$ of generators of μ_{p^n} corresponds to an isomorphism $\varprojlim \mathbb{Z}_p[\mu_{p^n}] \cong \mathbb{Z}_p[[T]]$. Let

$$\rho : \Pi_{\mathbb{Q}(\mu_{p^\infty})} \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}_p[[T]]\right)$$

be the representation obtained with respect to this isomorphism by the compatibility of the various representations ρ_n. Since $\mathrm{Im}\rho_n \subset \mathrm{GL}_2\left(\mathbb{Z}_p[\gamma_n + \gamma_n^{-1}]\right)$, the image of ρ lies in $\mathrm{GL}_2\left(\mathbb{Z}_p[[(1+T)+(1+T)^{-1}]]\right)$. In fact, we have

$$\rho(\sigma_0) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \rho(\sigma_1) = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix} \tag{4.39}$$

for some $\alpha \in \mathbb{Z}_p[[T]]^\times$; moreover, from the proof of Proposition 4.37, α satisfies $2 + \alpha = -(1+T) - (1+T)^{-1}$, and hence

$$\begin{aligned} \alpha &= -3 - T - (1+T)^{-1} \\ &= -3 - T - (1 - T + T^2 - \cdots) \\ &= -4 - T^2 + T^3 - \cdots . \end{aligned} \tag{4.40}$$

We claim that there is a $\mathbb{Z}_p$-algebra automorphism ψ of $\mathbb{Z}_p[[T]]$ which takes $\mathbb{Z}_p[[T^2]]$ to $\mathbb{Z}_p[[(1+T)+(1+T)^{-1}]] = \mathbb{Z}_p[[T^2 - T^3 + T^4 - \cdots]]$. Let $f(T) = a_1 T + a_2 T^2 + \cdots \in \mathbb{Z}_p[[T]]$ be a square root of $T^2 - T^3 + T^4 - \cdots$; for example, let $a_1 = 1$, and define each a_n recursively by

$$a_n = \frac{1}{2}\left((-1)^{n+1} - \sum_{\substack{2 \le i,j \le n-1 \\ i+j=n+1}} a_i a_j \right).$$

Let ψ be the $\mathbb{Z}_p$-algebra endomorphism taking T to $f(T)$. Then ψ is injective, and induces a surjective map on cotangent spaces. Therefore, ψ is an isomorphism, as claimed.

Composing ρ with the automorphism of $\mathrm{GL}_2(\mathbb{Z}_p[[T]])$ induced from ψ^{-1} gives a representation

$$\rho' : \Pi_{\mathbb{Q}(\mu_{p^\infty})} \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}_p[[T^2]]\right)$$

which satisfies

$$\rho'(\sigma_0) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \rho'(\sigma_1) = \begin{pmatrix} 1 & 0 \\ -4 - T^2 & 1 \end{pmatrix}.$$

Let $\bar{\rho}$ be the representation obtained from ρ' by reducing $\bmod (p, T^2)$, so that $\bar{\rho}$ is the representation associated to the p-torsion points of the Legendre family of elliptic curves, and let $S = \{\sigma_0, \sigma_1\}$.

Theorem 4.41 *As a representation over $\mathbb{Z}_p[[T^2]] \cong \mathbb{Z}_p[[T]]$, $\rho'|_{\Pi_{\overline{\mathbb{Q}}}}$ is a representative of the S-ordinary universal deformation $[\rho^{\mathrm{univ}}_{S-\mathrm{ord}}]$ of $\bar{\rho}$.*

Proof: The universal property of $[\rho^{\mathrm{univ}}_{S-\mathrm{ord}}]$ gives a $\mathbb{Z}_p$-algebra homomorphism

$$\phi : \mathbb{Z}_p[[T]] \longrightarrow \mathbb{Z}_p[[T^2]]$$

which takes $[\rho^{\mathrm{univ}}_{S-\mathrm{ord}}]$ to $[\rho'|_{\Pi_{\overline{\mathbb{Q}}}}]$. From the proof of Theorem 2.31, $\phi(T) = T^2$, so ϕ is an isomorphism. $\square$

Remark: The representation ρ' arises naturally as a representation of the larger Galois group $\Pi_{\mathbb{Q}(\mu_{p^\infty})}$. Since the image of $\bar{\rho}(\sigma_i)$ has order dividing $2p$

for each $i = 0, 1, \infty$, by Theorem 3.12, $\rho^{\mathrm{univ}}_{S-\mathrm{ord}}$ can be extended to a representation of $\Pi_{\mathbb{Q}(\mu_{p^\infty})}$; therefore, up to multiplication by a representation $\chi : G_{\mathbb{Q}(\mu_{p^\infty})} \longrightarrow \mathbb{Z}_p[[T^2]]^\times$, ρ' is the composition of this extension of $\rho^{\mathrm{univ}}_{S-\mathrm{ord}}$ with the map induced from ϕ.

5 Relation to Ihara's Cocycle

5.1 Ihara's Construction

We define a $\mathbb{Z}_p$-algebra $\mathcal{A}$ by

$$\mathcal{A} := \mathbb{Z}_p[[t_0, t_1, t_\infty]] \big/ \left((t_0+1)(t_1+1)(t_\infty+1)-1\right).$$

In [Iha86b], Ihara constructs a cocycle

$$F : G_{\mathbb{Q}} \longrightarrow \mathcal{A}^\times$$

which describes, for each n, the action of $G_{\mathbb{Q}(\mu_{p^n})}$ on the primitive quotients of the Jacobian of the Fermat curve

$$F_n : x^{p^n} + y^{p^n} = 1.$$

We briefly describe Ihara's original construction.

Fix a prime p, and let $\mathcal{F}$ be the pro-p completion of the free group on two generators g_0, g_1. Let $g_\infty = (g_0 g_1)^{-1}$, and let $\mathcal{M}$ be the maximal algebraic pro-p extension of $\mathbb{Q}(t)$ unramified outside $\{0, 1, \infty\}$. Fix an isomorphism $\iota : \mathcal{F} \longrightarrow \mathrm{Gal}\left(\mathcal{M}/\overline{\mathbb{Q}}(t)\right)$ such that for each $i = 0, 1, \infty$, g_i is mapped to a topological generator of an inertia group above i. The choice of such an isomorphism ι gives rise to a representation of $G_{\mathbb{Q}}$ in the group of outer automorphisms of $\mathcal{F}$. More precisely, let A be the subgroup of $\mathrm{Aut}(\mathcal{F})$ consisting of those automorphisms σ for which there is some $\alpha \in \mathbb{Z}_p^\times$ satisfying $\sigma(g_i) \sim g_i^\alpha$ for each $i = 0, 1, \infty$. An automorphism of a group G is said to be an *inner automorphism* if it arises as conjugation by some element of G. We denote by $\mathrm{Int}(G)$ the group of inner automorphisms of G, and by $\mathrm{Out}(G)$ the group $\mathrm{Aut}(G)/\mathrm{Int}(G)$ of *outer automorphisms* of G.

Definition 5.1 *The* pro-p braid group (*of degree* 2) *is the group*

$$\Phi := A/\mathrm{Int}(\mathcal{F}).$$

Given $\gamma \in G_{\mathbb{Q}} \cong \mathrm{Gal}\left(\mathcal{M}/\mathbb{Q}(t)\right)/\mathrm{Gal}\left(\mathcal{M}/\overline{\mathbb{Q}}(t)\right)$, choose a lift $\tilde{\gamma}$ of γ to $\mathrm{Gal}\left(\mathcal{M}/\mathbb{Q}(t)\right)$. Conjugation by $\tilde{\gamma}$ defines an automorphism of $\mathrm{Gal}\left(\mathcal{M}/\mathbb{Q}(t)\right)$ whose reduction modulo $\mathrm{Int}\left(\mathrm{Gal}\left(\mathcal{M}/\mathbb{Q}(t)\right)\right)$ depends only on γ. By the isomorphism ι, we obtain an outer automorphism σ_γ of $\mathcal{F}$. Moreover, by Theorem 3.1, σ_γ is an element of Φ; thus the assignment $\gamma \mapsto \sigma_\gamma$ defines a representation

$$\phi : G_{\mathbb{Q}} \longrightarrow \Phi.$$

Let $\mathcal{F}'' = [[\mathcal{F},\mathcal{F}],[\mathcal{F},\mathcal{F}]]$ denote the double commutator subgroup of $\mathcal{F}$. Let Ψ denote the image of Φ in $\mathrm{Out}\left(\mathcal{F}/\mathcal{F}''\right)$ under the canonical homomorphism $r : \mathrm{Out}(\mathcal{F}) \longrightarrow \mathrm{Out}\left(\mathcal{F}/\mathcal{F}''\right)$. In [Iha86b], Ihara studies the representation

$$\psi : G_{\mathbb{Q}} \longrightarrow \Psi$$

obtained by composing ϕ with r.

The quotient $\mathcal{F}/\mathcal{F}'$ is isomorphic to the pro-p completion of the abelianization of the free group on two generators; that is, $\mathcal{F}/\mathcal{F}'$ is isomorphic to the pro-p completion $\mathbb{Z}_p \times \mathbb{Z}_p$ of the free abelian group $\mathbb{Z} \times \mathbb{Z}$ on two generators.

Since $\mathcal{F}'/\mathcal{F}''$ is abelian, the automorphism of $\mathcal{F}'/\mathcal{F}''$ given by conjugation by any element $g \in \mathcal{F}$ depends only on the reduction of $g \mod \mathcal{F}'$; thus $\mathcal{F}/\mathcal{F}'$ acts by conjugation on $\mathcal{F}'/\mathcal{F}''$. The group $\mathcal{F}'/\mathcal{F}''$ is an abelian pro-p group, and hence is endowed with a canonical action of $\mathbb{Z}_p$. Therefore, $\mathcal{F}'/\mathcal{F}''$ is a module over

$$\mathbb{Z}_p[[\mathcal{F}/\mathcal{F}']] \cong \mathbb{Z}_p[[\mathbb{Z}_p \times \mathbb{Z}_p]] \cong \mathbb{Z}_p[[u,v]] \cong \mathcal{A}.$$

Fixing the isomorphism $\mathbb{Z}_p[[\mathcal{F}/\mathcal{F}']] \longrightarrow \mathcal{A}$ which maps g_i to $t_i + 1$ for each $i = 0, 1, \infty$, $\mathcal{F}'/\mathcal{F}''$ obtains the structure of an $\mathcal{A}$-module in such a way that multiplication by $t_i + 1$ is given by conjugation by g_i for each $i = 0, 1, \infty$.

Theorem 5.2 *This action of $\mathcal{A}$ makes $\mathcal{F}'/\mathcal{F}''$ into a free $\mathcal{A}$-module of rank one generated by $[g_0, g_1]$.*

Proof: See [Iha86b], §II, Theorem 2. $\square$

Let $\chi_p : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_p^\times$ denote the p-cyclotomic character, which describes the action of $G_{\mathbb{Q}}$ on $\mu_{p^\infty} \subset \overline{\mathbb{Q}}$. The group $G_{\mathbb{Q}}$ acts as $\mathbb{Z}_p$-algebra automorphisms on $\mathcal{A}$ by

$$\gamma \cdot (1 + t_i) = (1 + t_i)^{\chi_p(\gamma)}$$

for each $\gamma \in G_{\mathbb{Q}}$, and each $i = 0, 1, \infty$. For $\gamma \in G_{\mathbb{Q}}$, let $F_\gamma(t_0, t_1, t_\infty) \in \mathcal{A}^\times$ be the unique element satisfying

$$\psi(\gamma)\left([g_0, g_1]\right) = F_\gamma(t_0, t_1, t_\infty) \cdot [g_0, g_1].$$

Proposition 5.3 *The assignment $\gamma \longmapsto F_\gamma$ defines a continuous 1-cocycle*

$F : G_{\mathbb{Q}} \longrightarrow \mathcal{A}^{\times}$.

Proof: See [Iha86b], §II, Theorem 3B(ii). $\square$

Since $G_{\mathbb{Q}(\mu_{p^\infty})}$ acts trivially on $\mathcal{A}$, the restriction of F to $G_{\mathbb{Q}(\mu_{p^\infty})}$ is a homomorphism, which we also denote by F.

Let $a, b \in \mathbb{Z}/p^n\mathbb{Z} \setminus \{0\}$ be such that at least one of a, b is a unit in $\mathbb{Z}/p^n\mathbb{Z}$, and let $c = -(a+b)$. Let a_n (respectively b_n, c_n) denote the integer in $\{0, 1, \ldots, p^n - 1\}$ reducing to a (resp. b, c) $\mod p^n$. The Jacobian $J_n^{(a,b,c)}$ of the complete nonsingular model of the curve

$$C_n^{(a,b,c)} : x^{p^n} = y^{a_n}(y-1)^{b_n}$$

has a quotient $A_n^{(a,b,c)}$ which contains $\mathbb{Z}[\zeta_n]$ in its endomorphism ring, where the action of ζ_n on $A_n^{(a,b,c)}$ arises from the action of μ_{p^n} on $C_n^{(a,b,c)}$ given by $\zeta_n \cdot (x, y) = (\zeta_n x, y)$ for a generator ζ_n of μ_{p^n} (see [Iha86b], p.76). In fact, the Tate module $T_p\left(A_n^{(a,b,c)}\right)$ is a free module of rank one over $\mathbb{Z}_p[\zeta_n]$, and the action of $G_{\mathbb{Q}(\mu_{p^n})}$ on $T_p\left(A_n^{(a,b,c)}\right)$ commutes with the action of $\mathbb{Z}_p[\zeta_n]$. Therefore, the action of $\gamma \in G_{\mathbb{Q}(\mu_{p^n})}$ is given by multiplication by some element $F_{\gamma,n}^{(a,b,c)} \in \mathbb{Z}_p[\zeta_n]^{\times}$.

Theorem 5.4 (Ihara, 1986) *For each $\gamma \in G_{\mathbb{Q}(\mu_{p^n})}$, $F_{\gamma,n}^{(a,b,c)}$ is equal to $F_\gamma\left(\zeta_n^a - 1, \zeta_n^b - 1, \zeta_n^c - 1\right)$.*

Proof: See [Iha86b], §II, Theorem 4 and its corollary. $\square$

For each n, let J_n denote the Jacobian of the Fermat curve F_n. Then J_n is isogenous to the sum of J_{n-1} together with each $A_n^{(a,b,c)}$, where exactly one triple (a, b, c) is chosen from each set $\{(ka, kb, kc)\}_{k \in (\mathbb{Z}/p^n\mathbb{Z})^{\times}}$ (see [Iha86b], p.78). On the other hand, under the isomorphism ι, the commutator subgroup $\mathcal{F}'$ corresponds to the subfield $\mathcal{M}' = \bigcup_n K_n$, where K_n is the function field of F_n, and the subgroup $\mathcal{F}''$ corresponds to $\mathcal{M}'' = \bigcup_n K_n^{\mathrm{unrab}}$, where K_n^{unrab} denotes the maximal unramified abelian pro-p extension of K_n. Thus we have the following tower of extensions:

$$
\begin{tikzcd}
\mathcal{M} \arrow[d, dash, "\mathcal{F}''"] \\
\mathcal{M}'' = \bigcup_{n\in\mathbb{N}} K_n^{\mathrm{unrab}} \arrow[d, dash, "\mathcal{F}'/\mathcal{F}''"] \arrow[dd, dash, bend right=60, "\mathcal{F}/\mathcal{F}''"'] \\
\mathcal{M}' = \bigcup_{n\in\mathbb{N}} K_n \arrow[d, dash, "\mathcal{F}/\mathcal{F}'"] \\
\overline{\mathbb{Q}}(t)
\end{tikzcd}
$$

An *isogeny* of abelian varieties is a surjective homomorphism of abelian varieties whose kernel is finite. Subgroups H of the Tate module $T_p(J_n)$ of finite index are in one-to-one correspondence with isogenies $f_H : J \longrightarrow J_n$ in such a way that $f_H(T_p(J_n)) = H$. By geometric class field theory, such isogenies are in one-to-one correspondence with finite unramified abelian coverings $C_H \longrightarrow F_n$ in such a way that

$$\mathrm{Gal}\left(\overline{\mathbb{Q}}(C_H)/\overline{\mathbb{Q}}(F_n)\right) \cong T_p(J_n)/H,$$

where $\overline{\mathbb{Q}}(C_H), \overline{\mathbb{Q}}(F_n)$ are the function fields over $\overline{\mathbb{Q}}$ of C_H and F_n respectively (see [Ser88], Ch. VI, §2, Proposition 10 and the corollary to Proposition 11). Therefore, letting $\mathcal{S}_n$ denote the set of finite unramified abelian extensions

K_n, we have

$$\begin{aligned}
\mathrm{Gal}\left(K_n^{\mathrm{unrab}}/K_n\right) &= \varprojlim_{L\in\mathcal{S}_n} \mathrm{Gal}\left(L/K_n\right) \\
&= \varprojlim_{\substack{H\subset T_p(J_n)\\ \text{finite index}}} \mathrm{Gal}\left(\overline{\mathbb{Q}}(C_H)/K_n\right) \\
&\cong \varprojlim_{\substack{H\subset T_p(J_n)\\ \text{finite index}}} (T_p(J_n)/H) = T_p(J_n),
\end{aligned}$$

so $T_p(J_n)$ is isomorphic to $\mathrm{Gal}\left(K_n^{\mathrm{unrab}}/K_n\right)$. Thus one might expect the homomorphism F with the property of Theorem 5.4 to arise from the representation Ψ.

5.2 The Inertia Group at Infinity

Let $\rho : \Pi_{\mathbb{Q}(\mu_{p^\infty})} \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}_p[[T]]\right)$ be as in §4.8, and for any uniformizer π at ∞, let $\mathbb{Q}_\pi(\mu_{p^\infty}) = \mathbb{Q}(\mu_{p^\infty})((\pi))$. Restricting ρ to the inertia subgroup I_∞ at ∞ gives a representation ρ_∞ of $I_\infty = \mathrm{Gal}(M_\infty/\mathbb{Q}_\pi(\mu_{p^\infty}))$, where $M_\infty := \bigcup_n \overline{\mathbb{Q}(\mu_{p^\infty})}\left(\left(\pi^{1/n}\right)\right)$. The tower

$$\begin{array}{c}
M_\infty \\
\Big| \, {\scriptstyle G_{\mathbb{Q}(\mu_{p^\infty})}} \\
\bigcup_n \mathbb{Q}(\mu_{p^\infty})\left(\left(\pi^{1/n}\right)\right) \\
\Big| \\
\mathbb{Q}_\pi(\mu_{p^\infty})
\end{array}$$

gives an inclusion $\iota_\pi : G_{\mathbb{Q}(\mu_{p^\infty})} \hookrightarrow I_\infty$ which depends on the choice of uniformizer π. Restricting ρ_∞ to the image of ι_π thus gives a representation

$$\rho_{\infty,\pi} : G_{\mathbb{Q}(\mu_{p^\infty})} \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}_p[[T]]\right).$$

Let $p_n : \mathrm{GL}_2\left(\mathbb{Z}_p[[T]]\right) \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}_p[\mu_{p^n}]\right)$ be the map induced from the ring homomorphism $\mathbb{Z}_p[[T]] \longrightarrow \mathbb{Z}_p[\mu_{p^n}]$ taking T to $\gamma_n - 1$; since ρ was obtained by the isomorphism $\varprojlim \mathbb{Z}_p[\mu_{p^n}] \cong \mathbb{Z}_p[[T]]$ taking $(\gamma_n - 1)_{n\in\mathbb{N}}$ to T, we have $\rho_n^- \otimes \mathbb{Z}_p[\mu_{p^n}] = p_n \circ \rho$.

Fixing the uniformizer $\pi = 1/16t$, and letting $u = (1/16t)^{1/2p^n}$, C_n^- is isomorphic over $\mathbb{Q}((u))$ to the curve

$$\tilde{C}_n^- : y^2 = x \prod_{j=1}^{\frac{p^n-1}{2}} \left(1 + (\zeta_n^j + \zeta_n^{-j} - 2)u^4x^2\right) + \frac{x^{p^n+1}}{4} - 2u^{2p^n}x^{p^n+1}$$

by the map $\tilde{C}_n^- \longrightarrow C_n^-$ taking (x, y) to $\left(\frac{1}{u^2x}, \frac{y}{u^{p^n}x^{\frac{p^n+1}{2}}}\right)$. The curve $\tilde{C}_n^-$ has good reduction at $u = 0$, and gives the reduced curve

$$\bar{C}_n^- : y^2 = \frac{x^{p^n+1}}{4} + x.$$

On the other hand, the curve $C_n^{(1,1,p^n-2)}$ considered by Ihara when $a = b = 1$ is given by

$$C_n^{(1,1,p^n-2)} : y(y-1) = x^{p^n},$$

and there is an isomorphism $\psi : \bar{C}_n^- \longrightarrow C_n^{(1,1,p^n-2)}$ given by

$$\psi : (x, y) \longmapsto \left(\frac{1}{x}, \frac{y}{x^{\frac{p^n+1}{2}}} + \frac{1}{2}\right).$$

The endomorphism $\gamma_n + \gamma_n^{-1}$ of J_n^- gives rise to a corresponding endomorphism of the Jacobian $\bar{J}_n^-$ of $\bar{C}_n^-$, and the reduction map

$$J_n^- \left(\overline{\mathbb{Q}_\pi(\mu_{p^\infty})}\right) \longrightarrow \bar{J}_n^- \left(\overline{\mathbb{Q}(\mu_{p^\infty})}\right)$$

induces a $\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]$-module isomorphism $V_p(J_n^-) \cong V_p(\bar{J}_n^-)$. Counting $\mathbb{Q}_p$-dimensions shows that under the isomorphism of Jacobians induced from ψ, the quotient $A_n^{(1,1,p^n-2)}$ of $J_n^{(1,1,p^n-2)}$ must correspond to a quotient A_n of $\bar{J}_n^-$ such that the extended Tate module $V_p(A_n)$ corresponds to the unique $\mathbb{Q}_p[\gamma_n + \gamma_n^{-1}]$-module quotient of $V_p(\bar{J}_n^-)$ isomorphic to $\mathbb{Q}_p(\zeta_n + \zeta_n^{-1})^2$.

The endomorphism $\gamma_n + \gamma_n^{-1}$ of the Jacobian of $\tilde{C}_n^-$ arises from the action of μ_{p^n} on C_n via the map

$$\begin{aligned} C_n &\longrightarrow \tilde{C}_n^- \\ (x, y) &\longmapsto \left(\frac{1}{(x + x^{-1})u^2}, \frac{y}{ux^{\frac{p^n+1}{2}}(x + x^{-1})^{\frac{p^n+1}{2}}}\right), \end{aligned}$$

where $u^{2p^n} = \pi$. If $P_1 = (x, y) \in C_n$ is a preimage of $Q = (w, z) \in \tilde{C}_n^-$, then so is $P_2 = \left(\frac{1}{x}, \frac{y}{x^{p^2+1}}\right)$; applying γ_n to P_1, P_2 and mapping to $\tilde{C}_n^-$ gives the points

$$\begin{aligned} Q_1 &= \left(\frac{\zeta_n x}{(\zeta_n^2 x^2 + 1)u^2}, \frac{y}{u(\zeta_n x^2 + \zeta_n^{-1})^{\frac{p^n+1}{2}}}\right), \\ Q_2 &= \left(\frac{\zeta_n x}{(\zeta_n^2 + x^2)u^2}, \frac{y}{u(\zeta_n + \zeta_n^{-1} x^2)^{\frac{p^n+1}{2}}}\right). \end{aligned}$$

Projectivizing these points and specializing at $u = 0$ gives the point at infinity

$(0 : 1 : 0)$ on $\bar{C}_n^-$ if $v_u(x) < 2$, where v_u denotes the u-adic valuation. If $v_u(x) \geq 2$, then $v_u(y) \geq 1$. Letting $x' = x/u^2$, $y' = y/u$, specializing gives the points $\bar{Q}_1 = \left(\zeta_n \bar{x}', \zeta_n^{\frac{p^n+1}{2}} \bar{y}'\right)$ and $\bar{Q}_2 = \left(\zeta_n^{-1} \bar{x}', \zeta_n^{-\frac{p^n+1}{2}} \bar{y}'\right)$ respectively, where $\bar{x}'$, $\bar{y}'$ denote the reductions of x, $y \mod u$. Therefore, the action of $\gamma_n + \gamma_n^{-1}$ on $\bar{J}_n^-$ obtained from that on $\tilde{J}_n^-$ is precisely that considered by Ihara arising from the action of μ_{p^n} on $\bar{C}_n^-$ by $\gamma_n(x, y) = \left(\zeta_n x, \zeta_n^{\frac{p^n+1}{2}} y\right)$. In particular, $T_p(A_n)$ is a free $\mathbb{Z}_p[\zeta_n]$-module of rank one, and thus also a free $\mathbb{Z}_p[\zeta_n + \zeta_n^{-1}]$-module of rank two. Moreover, writing

$$\rho_{\infty,\pi}(\sigma) = M_\sigma(T) \in \mathrm{GL}_2\left(\mathbb{Z}_p[[(1+T) + (1+T)^{-1}]]\right)$$

for each $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$, the representation

$$\rho_{\infty,n} : G_{\mathbb{Q}(\mu_{p^\infty})} \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}_p[\zeta_n + \zeta_n^{-1}]\right)$$

given by $\rho_{\infty,n}(\sigma) = M_\sigma(\zeta_n - 1)$ is the Galois representation associated to $T_p(A_n)$ as a $\mathbb{Z}_p[\zeta_n + \zeta_n^{-1}]$-module.

Let $F : G_{\mathbb{Q}(\mu_{p^\infty})} \longrightarrow \mathcal{A}^\times$ be Ihara's representation. There is a $\mathbb{Z}_p$-algebra isomorphism $\theta : \mathcal{A} \longrightarrow \mathbb{Z}_p[[u, v]]$ which takes t_0 to u and t_1 to v. Let

$$r : \mathbb{Z}_p[[u, v]] \longrightarrow \mathbb{Z}_p[[T]]$$

be the $\mathbb{Z}_p$-algebra homomorphism such that $r(u) = r(v) = T$, and let $\bar{F} = r \circ \theta \circ F$. Since $r \circ \theta(t_\infty) = (T+1)^{-2} - 1$, we have

$$F_\sigma(\zeta_n - 1, \zeta_n - 1, \zeta_n^{-2} - 1) = \bar{F}_\sigma(\zeta_n - 1)$$

for each $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$; hence letting $\bar{p}_n : \mathbb{Z}_p[[T]] \longrightarrow \mathbb{Z}_p[\zeta_n]$ denote the homomorphism taking T to $\zeta_n - 1$, $\bar{p}_n \circ \bar{F}$ is the representation of $G_{\mathbb{Q}(\mu_{p^\infty})}$ associated to $A_n^{(1,1,p^n-2)}$.

In order to obtain the representation $\bar{F}$ from $\rho_{\infty,\pi}$, we first need some lemmas:

Lemma 5.5 *Let V be a free $\mathbb{Z}_p[\zeta_n]$-module of rank one, and let σ be the automorphism of V given by multiplication by $\alpha \in \mathbb{Z}_p[\zeta_n]^\times$. Let δ be the nontrivial element of* $\mathrm{Gal}\,(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p(\zeta_n+\zeta_n^{-1}))$*. Then the eigenvalues of $\sigma \otimes_{\mathbb{Z}_p[\zeta_n+\zeta_n^{-1}]} \mathbb{Z}_p[\zeta_n]$ are α and α^δ.*

Proof: Let $\{v\}$ be a $\mathbb{Z}_p[\zeta_n]$-basis for V. Fix the $\mathbb{Z}_p[\zeta_n+\zeta_n^{-1}]$-basis $\{v, \zeta_n v\}$ for V, and let $\alpha_0, \alpha_1 \in \mathbb{Z}_p[\zeta_n+\zeta_n^{-1}]$ be such that $\alpha = \alpha_0 + \zeta_n\alpha_1$. Since

$$\begin{aligned} \sigma(v) &= \alpha v = \alpha_0 v + \alpha_1\zeta_n v \\ \text{and} \qquad \sigma(\zeta_n v) &= \alpha\zeta_n v = \zeta_n^2\alpha_1 v + \alpha_0\zeta_n v \\ &= -\alpha_1 v + \left(\alpha_0 + (\zeta_n+\zeta_n^{-1})\alpha_1\right)\zeta_n v, \end{aligned}$$

σ is given by $\left(\begin{smallmatrix} \alpha_0 & -\alpha_1 \\ \alpha_1 & \alpha_0+(\zeta_n+\zeta_n^{-1})\alpha_1 \end{smallmatrix}\right)$ relative to the basis $\{v, \zeta_n v\}$. In particular, the characteristic polynomial f_σ of σ is given by

$$\begin{aligned} f_\sigma(X) &= X^2 - \left(2\alpha_0 + (\zeta_n+\zeta_n^{-1})\alpha_1\right)X + \left(\alpha_0^2 + (\zeta_n+\zeta_n^{-1})\alpha_0\alpha_1 + \alpha_1^2\right) \\ &= \left(X - (\alpha_0+\zeta_n\alpha_1)\right)\left(X - (\alpha_0+\zeta_n^{-1}\alpha_1)\right) \\ &= (X-\alpha)(X-\alpha^\delta), \end{aligned}$$

as desired. $\square$

Lemma 5.6 *The representation $\rho_{\infty,\pi}$ is conjugate to an upper-triangular representation.*

Proof: Let χ denote the cyclotomic character. For $\gamma \in I_\infty$, we have $\gamma\sigma_\infty\gamma^{-1} = \sigma_\infty^{\chi(\gamma)}$, and thus $\rho(\gamma)\rho(\sigma_\infty)\rho(\gamma)^{-1} = \rho(\sigma_\infty)^{\chi(\gamma)}$. Since $\rho(\sigma_\infty)$ has order dividing $2p^k$ for some k in every finite quotient of $\mathrm{GL}_2(\mathbb{Z}_p[[T]])$, we have $\rho(\sigma_\infty)^{\chi(\gamma)} = \rho(\sigma_\infty)^{\chi_p(\gamma)}$, where $\chi_p : G_\mathbb{Q} \longrightarrow \mathbb{Z}_p^\times$ denotes the p-cyclotomic character which describes the action of $G_\mathbb{Q}$ on $\mu_{p^\infty} \subset \overline{\mathbb{Q}}$. The group I_∞ is contained in $\Pi_{\mathbb{Q}(\mu_{p^\infty})}$, so γ fixes μ_{p^∞} pointwise; thus $\chi_p(\gamma) = 1$, and hence $\rho(\gamma)\rho(\sigma_\infty)\rho(\gamma)^{-1} = \sigma_\infty$. In particular, the image of $\rho_{\infty,\pi}$ is contained in the centralizer $Z_{\mathrm{GL}_2(\mathbb{Z}_p[[T]])}(\rho(\sigma_\infty))$ of $\rho(\sigma_\infty)$ in $\mathrm{GL}_2(\mathbb{Z}_p[[T]])$. If we show that the non-scalar matrix $\rho(\sigma_\infty)$ is upper-triangular, then its centralizer must also be upper-triangular, thus proving the lemma.

From 4.39 and 4.40, we have

$$\rho(\sigma_\infty) = \begin{pmatrix} 1 & -1 \\ 2 + (1+T) + (1+T)^{-1} & -1 - (1+T) - (1+T)^{-1} \end{pmatrix}.$$

For any $g(T) \in \mathbb{Z}_p[[T]]^\times$, applying Hensel's lemma to $X^2 - g(T)$ shows that $g(T)$ is a square in $\mathbb{Z}_p[[T]]$ if and only if its reduction mod (p, T) is a square in $\mathbb{F}_p$. Thus $g_1(T) := 2+(1+T)+(1+T)^{-1}$ and $g_2(T) := g_1(T)-4 = T^2(1+T)^{-1}$ are both squares in $\mathbb{Z}_p[[T]]$ since $g_1(T)$ reduces to $4 \in \mathbb{F}_p$ and $g_2(T)/T^2$ reduces to $1 \in \mathbb{F}_p$. Let $g(T) \in \mathbb{Z}_p[[T]]$ be a square root of $g_1(T)g_2(T)$, and let

$$h(T) := \tfrac{1}{2}\left(g_1(T)^2 + g(T)\right).$$

Conjugating $\rho(\sigma_\infty)$ by the matrix $M = \left(\begin{smallmatrix} 1 & 0 \\ h(T) & 1 \end{smallmatrix}\right)$ gives

$$M\rho(\sigma_\infty)M^{-1} = \begin{pmatrix} h(T)+1 & -1 \\ 0 & 1-h(T)-g_1(T) \end{pmatrix},$$

as desired. □

Identify $\rho_{\infty,\pi}$ with any one of its upper-triangular conjugates, and let $f_1, f_2 : G_{\mathbb{Q}(\mu_{p^\infty})} \longrightarrow \mathbb{Z}_p[[T]]^\times$ be such that for each $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$,

$$\rho_{\infty,\pi}(\sigma) = \begin{pmatrix} (f_1)_\sigma(T) & * \\ 0 & (f_2)_\sigma(T) \end{pmatrix}.$$

Theorem 5.7 *One of f_1 or f_2 is equal to $\bar{F}$; the other is uniquely determined by the property that the image of each $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$ gives $\bar{F}(\zeta_n - 1)^\delta$ when evaluated at $\zeta_n - 1$.*

Proof: Given $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$, by Lemmas 5.5 and 5.6, the action of σ on $T_p(A_n)$ as a $\mathbb{Z}_p[\zeta_n]$-module is given by multiplication by $(f_{j(n)})\sigma(\zeta_n - 1)$ for some $j(n) = 1$ or 2. On the other hand, since A_n is isomorphic to $A_n^{(1,1,p^n-2)}$ over $\mathbb{Q}(\mu_{p^\infty})$, σ acts on $T_p(A_n)$ by multiplication by $\bar{F}_\sigma(\zeta_n - 1)$. Therefore, for some $j = 1$ or 2, $(\bar{F}_\sigma - (f_j)_\sigma)(\zeta_n - 1) = 0$ for infinitely many n. It follows from the Weierstrass Preparation Theorem that a nonzero power series can have only a finite number of zeroes $z \in \overline{\mathbb{Q}}_p$ satisfying $|z| < 1$, where $|\cdot|$ is the p-adic norm (see [Was82], Corollary 7.2). Therefore, $\bar{F}_\sigma = (f_j)_\sigma$. Since $\bar{F}, f_1, f_2$ are homomorphisms, we have $\bar{F} = f_k$ for some $k = 1$ or 2. The final statement follows from Lemma 5.5 together with the corollary of the Weierstrass Preparation Theorem used above. □

Remark: Which f_k is equal to $\bar{F}$ depends on the choice of conjugate of $\rho_{\infty,\pi}$. Since $\rho_{\infty,\pi}$ describes the action of $G_{\mathbb{Q}(\mu_{p^\infty})}$ on $T_p(A_n)$ as a $\mathbb{Z}_p[\zeta_n+\zeta_n^{-1}]$-module, our construction does not distinguish which f_k is equal to $\bar{F}$.

6 Conclusion

In the preceding chapters, we have described a new construction of a specialization of Ihara's cocycle. This construction arises from the $\{\sigma_0, \sigma_1\}$-ordinary universal deformation of the residual representation $\bar{\rho}$ which describes the action of $\Pi_{\overline{\mathbb{Q}}}$ on the Legendre family of elliptic curves. This universal deformation was extended by the rigidity theorem to a representation ρ of $\Pi_{\mathbb{Q}(\mu_{p^\infty})}$. Using a geometric construction of ρ, we showed that a specialization of Ihara's cocycle appears when ρ is specialized at infinity (given a particular choice of uniformizer).

This work suggests a number of directions for further research. First of all, the σ_0-ordinary universal deformation ring of the residual representation $\bar{\rho}$ is $\mathbb{Z}_p[[u, v]] \cong \mathcal{A}$; thus we are led to the following question:

Question 1 Does the extended σ_0-ordinary universal deformation of $\bar{\rho}$ of Theorem 3.12 give rise to Ihara's full cocycle when specialized at infinity?

Let k be any field, and let $M_0, M_1, M_2 \in \mathrm{GL}_n(k)$ be matrices satisfying $M_0 M_1 M_2 = \mathrm{Id}_n$ which generate an irreducible subgroup of $\mathrm{GL}_n(k)$. By a theorem of Belyĭ, if one of M_0, M_1, or M_2 differs from a scalar matrix by a matrix of rank one, then the triple (M_0, M_1, M_2) is rigid in $\mathrm{GL}_n(k)$. Thus one would expect that subject to an appropriate "ordinariness" condition, the universal deformation $(R^{\mathrm{univ}}, \rho^{\mathrm{univ}})$ of a residual representation

$$\bar{\rho} : \Pi_{\overline{\mathbb{Q}}} \longrightarrow \mathrm{GL}_n(\mathbb{F}_p)$$

would be rigid; that is, the triple $\big(\rho^{\mathrm{univ}}(\sigma_0), \rho^{\mathrm{univ}}(\sigma_1), \rho^{\mathrm{univ}}(\sigma_\infty)\big)$ would be rigid in $\mathrm{GL}_n(R^{\mathrm{univ}})$. Therefore, one expects to be able to extend this ρ^{univ} to a representation ρ of $\Pi_{K(t)}$, where K is a given cyclotomic extension of $\mathbb{Q}(\mu_{p^\infty})$. Furthermore, since Katz' construction applies to rigid representations of arbitrary dimension, it should be possible to construct ρ geometrically, in a similar manner to the construction of Chapter 4.

Question 2 What effect would increasing the dimension of the residual representation have on our construction? In particular, would Ihara's cocycle still appear, or some (possibly nonabelian) variant?

If the group $\Pi_{\overline{\mathbb{Q}}}$ is replaced with another algebraic fundamental group Π in our construction, the universal deformation seems much less likely to be rigid. Since the number of topological generators of Π is in general greater than 2, it may be necessary to increase the dimension of the residual representation in order to obtain a rigid situation. Also, a further study of rigid m-tuples in $\mathrm{GL}_n(R^{\mathrm{univ}})$ would be required if this generalization is to succeed.

Question 3 Under what conditions could our construction be carried out if $\Pi_{\overline{\mathbb{Q}}}$ is replaced with some other algebraic fundamental group? Under those conditions, what cocycles appear?

Another direction arises from Ihara's generalization of his own construction of his cocycle. In [Iha86a], he considers different towers of étale coverings of $\mathbb{P}^1(\overline{\mathbb{Q}}) \setminus \{0, 1, \infty\}$ having certain properties, and for each such tower constructs a "universal" cocycle

$$\phi : G_{\mathbb{Q}} \longrightarrow \mathcal{A}^\times,$$

where $\mathcal{A}$ is a completed group ring $\mathbb{Z}_p[[\mathfrak{g}]]$, the group $\mathfrak{g}$ depending on the tower of coverings.

Question 4 Is it possible to generalize our construction to give other cocycles of Ihara?

In general, the algebra $\mathcal{A}$ is not a power series ring; thus it would be necessary to begin with an obstructed deformation problem, which could not arise from a residual representation of an algebraic fundamental group. Therefore, significant difficulties already appear in the first step of such a generalization.

References

[Arm97] M.A. Armstrong. *Basic Topology.* Springer-Verlag, New York, 1997.

[Bel80] G.V. Belyĭ. On Galois extensions of a maximal cyclotomic field. *Math. USSR Izvestija*, 14(2), 1980.

[Dar00] Henri Darmon. Rigid local systems, Hilbert modular forms and Fermat's last theorem. *Duke Math. J.*, 102(3):413–449, 2000.

[dL97] Bart de Smit and Hendrick W. Lenstra, Jr. Explicit construction of universal deformation rings. In G. Cornell, G. Stevens, and J.H. Silverman, editors, *Modular Forms and Fermat's Last Theorem (Boston, MA, 1995)*, pages 313–326, New York, 1997. Springer-Verlag.

[DM00] Henri Darmon and Jean-François Mestre. Courbes hyperelliptiques à multiplications réelles et une construction de Shih. *Canad. Math. Bull.*, 43(3):304–311, 2000.

[Gou] Fernando Q. Gouvêa. Deformations of Galois representations. Notes from a course given by the author during the summer of 1999, available at www.colby.edu/personal/fqgouvea/web.html.

[GS71] S. Greco and P. Salmon. *Topics in $\mathfrak{m}$-adic Topologies.* Springer-Verlag, Berlin, 1971.

[Gv80] Lothar Gerritzen and Marius van der Put. *Schottky Groups and Mumford Curves.* Number 817 in Lecture notes in mathematics. Springer-Verlag, Berlin, 1980.

[Har97] Robin Hartshorne. *Algebraic Geometry.* Springer-Verlag, New York, 1997.

[Iha86a] Yasutaka Ihara. On Galois representations arising from towers of coverings of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$. *Invent. Math.*, 86(3):427–459, 1986.

[Iha86b] Yasutaka Ihara. Profinite braid groups, Galois representations and complex multiplications. *Ann. of Math.* (2), 123(1):43–106, 1986.

[Isa94] I. Martin Isaacs. *Character Theory of Finite Groups.* Dover Publications, New York, 1994.

[JL93] Gordon James and Martin Liebeck. *Representations and Characters of Finite Groups.* Cambridge University Press, Cambridge, 1993.

[Kat90] Nicholas M. Katz. *Exponential Sums and Differential Equations.* Number 124 in Annals of Mathematics Studies. Princeton University Press, Princeton, 1990.

[Lan64] Serge Lang. *Introduction to Algebraic Geometry.* Interscience Publishers, New York, 1964.

[Lan83] Serge Lang. *Abelian Varieties.* Springer-Verlag, New York, 1983.

[Lan93] Serge Lang. *Algebra.* Addison-Wesley, Reading, MA, 3rd edition, 1993.

[Mat87] Heinrich Matzat. *Konstruktive Galoistheorie.* Number 1284 in Lecture Notes in Mathematics. Springer-Verlag, Berlin, 1987.

[Maz86] B. Mazur. Arithmetic on curves. *Bull. Amer. Math. Soc.* (*N.S.*), 14(2):207–259, 1986.

[Maz89] B. Mazur. Deforming Galois representations. In Y. Ihara, K. Ribet, and J.-P. Serre, editors, *Galois Groups over* $\mathbb{Q}$, number 16 in Math. Sci. Res. Inst. Publ., New York, 1989. Springer-Verlag.

[Maz97] B. Mazur. An introduction to the deformation theory of Galois representations. In G. Cornell, G. Stevens, and J.H. Silverman, editors, *Modular Forms and Fermat's Last Theorem* (*Boston*, *MA*, *1995*), pages 243–311, New York, 1997. Springer-Verlag.

[Mil86a] J.S. Milne. Abelian varieties. In G.Cornell and J.H. Silverman, editors, *Arithmetic Geometry*, pages 103–150, New York, 1986. Springer-Verlag.

[Mil86b] J.S. Milne. Jacobian varieties. In G.Cornell and J.H. Silverman, editors, *Arithmetic Geometry*, pages 167–212, New York, 1986. Springer-Verlag.

[MM99] Gunter Malle and Heinrich Matzat. *Inverse Galois Theory.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999.

[Mor96] Patrick Morandi. *Field and Galois Theory.* Springer-Verlag, New York, 1996.

[Mum70] David Mumford. *Abelian Varieties*. Oxford University Press, London, 1970.

[Ser68] Jean-Pierre Serre. *Corps Locaux*. Hermann, Paris, 2nd edition, 1968.

[Ser88] Jean-Pierre Serre. *Algebraic Groups and Class Fields*. Springer-Verlag, New York, 1988. Translation of the French edition.

[Ser92] Jean-Pierre Serre. *Topics in Galois Theory*. Jones and Bartlett, Boston, 1992.

[Sha72] Stephen S. Shatz. *Profinite Groups, Arithmetic, and Geometry*. Princeton University Press, Princeton, NJ, 1972.

[ST68] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math.*(2), 88:492–517, 1968.

[TTV91] W. Tautz, J. Top, and A. Verberkmoes. Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Can. J. Math.*, 43(5):1055–1064, 1991.

[Vol96] Helmut Volklein. *Groups as Galois Groups*. Cambridge University Press, Cambridge, 1996.

[Was82] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Springer-Verlag, New York, 1982.