Advanced Studies in Pure Mathematics 17, 1989
Algebraic Number Theory — in honor of K. Iwasawa
pp. 1–21

Explicit Universal Deformations of Galois Representations

N. Boston[1] and B. Mazur[2]

To K. Iwasawa on the occasion of his 70th birthday

Given a continuous absolutely irreducible representation

$$\bar{\rho}\colon G_{\boldsymbol{Q}} \longrightarrow GL_2(\boldsymbol{F}_p)$$

and a finite set of primes S which contains the primes of ramification for $\bar{\rho}$ and the prime number p, the notion of *universal deformation* for $(\bar{\rho}, S)$ was discussed in [M]. It was shown in [M] that there exists a complete noetherian local ring R with residue field $\boldsymbol{F}_p$, uniquely determined up to canonical isomorphism, and a lifting

$$\rho\colon G_{\boldsymbol{Q}} \longrightarrow GL_2(R)$$

of $\bar{\rho}$ (unique up to strict equivalence—see § 3.1 below) which is unramified outside S, and satisfies a universal property vis à vis all liftings of $\bar{\rho}$ to $GL_2(\mathscr{A})$ which are unramified outside S, where $\mathscr{A}$ ranges through the category of complete local noetherian rings with residue field $\boldsymbol{F}_p$.

For $S=\{p\}$ and a class of representations $\bar{\rho}$ ("special dihedral representations") the universal deformation ring R was shown to be a power series ring in 3 variables over $\boldsymbol{Z}_p$. If X is the "universal deformation space", i.e., the space of continuous homomorphisms from R to $\boldsymbol{Z}_p$, then X is a 3-dimensional analytic manifold over $\boldsymbol{Q}_p$ and for each $x \in X$ specialization of ρ yields a Galois representation

$$\rho_x\colon G_{\boldsymbol{Q}} \longrightarrow GL_2(\boldsymbol{Z}_p)$$

(determined up to strict equivalence) which is a lifting of $\bar{\rho}$ and is unramified outside S. One of the aims of [M] was to embark on a systematic study of certain "natural subspaces" in X: loci of points $x \in X$ such that

Received July 31, 1987.

[1] Partially supported by the Sloan Foundation.

[2] Partially supported by the National Science Foundation.

ρ_x satisfies some "natural" condition (e.g., the image of an inertia group at p under ρ_x contains an open subgroup of finite index in $SL_2(Z_p)$ etc.—see § 3.3 below). The objective of this study was to get a detailed view of the structure of these "natural subspaces" in the universal deformation space for a particular class of representations $\bar{\rho}$ in order to have some idea what to expect in more general contexts.

In [B] a different view of the problem of universal deformations was taken, where group-theoretic tools were developed with the aim of making the universal deformations more explicit. A number of applications were given there to universal deformation problems related to local and global Galois groups.

The object of the present paper is to take again a particular class of representations ("admissible S_3-representations"—see Chapter 2) and to apply the techniques of [B] to study the universal deformation space and the structure of its "natural subspaces". Thanks to these techniques the arguments employed here are much more direct than in [M] and the results are more explicit. A distinction between two types of admissible S_3-representations emerges ("generic" vs. "degenerate)" as relevant to the structure of "natural subspaces". In the "generic" case, we completely determine this structure (Proposition 13 below). We also produce numerical conditions which, in the case of special S_3-representations, are equivalent to the condition of "genericity". We make computations which assure us that these numerical conditions indeed hold in a large number of instances.

Contents

Chapter 1. The General Set-Up

1.1. Relative p-completions

If F is a field, let G_F denote the Galois group Gal $(\bar{F}/F)$ for $\bar{F}$ a choice of separable algebraic closure. In this article we *fix a prime number p*, and an algebraic closure $\bar{\boldsymbol{Q}}_p$ of $\boldsymbol{Q}_p$. We let $\bar{\boldsymbol{Q}}$ denote the algebraic closure of $\boldsymbol{Q}$ contained in $\bar{\boldsymbol{Q}}_p$, which gives us a continuous injective homomorphism,

$$(1.1) \qquad G_{\boldsymbol{Q}_p} \hookrightarrow G_{\boldsymbol{Q}}.$$

If

$$\bar{\rho}\colon G_{\boldsymbol{Q}} \longrightarrow GL_2(\boldsymbol{F}_p)$$

is a continous homomorphism, let

$$\bar{\rho}_p\colon G_{\boldsymbol{Q}_p} \longrightarrow GL_2(\boldsymbol{F}_p)$$

denote its composition with (1.1). Let N (resp. N_p) denote the kernel of $\bar{\rho}$ (resp., of $\bar{\rho}_p$). Let $L \subset \bar{\boldsymbol{Q}}$ denote the splitting field of $\bar{\rho}$, i.e., the fixed subfield of $\bar{\boldsymbol{Q}}$ under the action of N, and let $L_p \subset \bar{\boldsymbol{Q}}_p$ denote the splitting field of $\bar{\rho}_p$.

Now fix S a (finite) set of nonarchimedean places of L consisting of all places lying above some finite set of rational primes, including the prime p. Let L_v denote the completion of L at any place v. By our set-up, we have singled out a "chosen" place (call it v_1) in S defined by the property that $L_{v_1} = L_p$.

Let $H \subset N$ denote the closed characteristic subgroup such that the Galois group $P := N/H$ is the Galois group of the maximal pro-p extension field of L in $\bar{\boldsymbol{Q}}$ which is unramified outside S (ramification at the archimedean primes being allowed). Let $H_p \subset N_p$ denote the closed characteristic subgroup such that $P_p := N_p/H_p$ is the maximal pro-p quotient group of N_p. Then the subgroup $H \subset G_{\boldsymbol{Q}}$ (resp. $H_p \subset G_{\boldsymbol{Q}_p}$) is normal.

Definition 1. The group $G := G_{\boldsymbol{Q}}/H$ is called the p-completion of $G_{\boldsymbol{Q}}$ relative to $\bar{\rho}$ and S. The group $G_p := G_{\boldsymbol{Q}_p}/H_p$ is called the p-completion of $G_{\boldsymbol{Q}_p}$ relative to $\bar{\rho}_p$.

Remark. The deformation-theoretic motivation for relative p-completions comes from the fact that ker $(GL_2(\mathscr{A}) \to GL_2(\boldsymbol{F}_p))$ is a pro-p-group (see [B], [M]) and so, for example, every lift $\rho\colon G_{\boldsymbol{Q}_p} \to GL_2(\mathscr{A})$ of $\bar{\rho}_p$, where $\mathscr{A}$ is a complete noetherian local ring with residue field $\boldsymbol{F}_p$, factors through the quotient group G_p.

By construction, we have the following diagram of pro-finite groups, where the horizontal lines are exact:

(1.2)
$$\begin{tikzcd}
1 \arrow[r] & P \arrow[r] & G \arrow[r] & A \arrow[r] & 1. \\
1 \arrow[r] & P_p \arrow[r] \arrow[u] & G_p \arrow[r] \arrow[u] & A_p \arrow[r] \arrow[u] & 1.
\end{tikzcd}$$

Here A (resp., A_p) is a finite group isomorphic to the image of $\bar{\rho}$ (resp., of $\bar{\rho}_p$) in $GL_2(\boldsymbol{F}_p)$.

If W is any topological group, we denote by $\bar{W}$ its p-Frattini quotient, i.e., $\bar{W}$ is the maximal elementary p-abelian topological quotient group of W.

By Local and Global Class Field Theory, the p-Frattini quotients $\bar{P}_p$ and $\bar{P}$ are finite. Since P_p and P are pro-p-groups, it then follows by Burnside's lemma ([K] Satz 4.10) that they are topologically finitely generated.

1.2. The p-Frattini quotients of P_p and of P

Suppose that A_p has order prime to p. Using the isomorphism provided by Local Class Field Theory we may induce an isomorphism of p-Frattini quotients

$$\bar{L}_p^* \xrightarrow[\cong]{} \bar{P}_p$$

viewed as $\boldsymbol{F}_p[A_p]$-modules. Let $\bar{P}_p^0 \subset \bar{P}_p$ denote the image of inertia; it is a sub $\boldsymbol{F}_p[A_p]$-module.

Proposition 1 ([I], [P]). *There are isomorphisms as $\boldsymbol{F}_p[A_p]$-modules:*

$$\bar{P}_p^0 \cong \boldsymbol{F}_p[A_p] \oplus \mu_p(L_p)$$
$$\bar{P}_p \cong \bar{P}_p^0 \oplus \boldsymbol{F}_p$$

where the second summand in the second line is given an $\boldsymbol{F}_p[A_p]$ structure via the trivial action of A_p.

Let E denote the group of ("global") units in the ring of integers of L and, if v is any nonarchimedean place, let E_v denote the group of ("local") units in the ring of integers of L_v. The natural mapping (provided by Global Class Field Theory) of the idèle class group of L to the Galois group of the maximal abelian extension of L induces a mapping on p-Frattini quotients $\oplus_{v \in S} \bar{E}_v \to \bar{P}$ which is equivariant for the action of A and whose kernel contains the image of $\bar{E}$, the p-Frattini quotient of the group of global units.

Definition 2. The pair (L, S) is called *neat* for p if

(a) The mapping $\bar{E}\to\oplus_{v\in S}\bar{E}_v$ is injective i.e., any global unit which is locally, for all $v\in S$, a p-th power, is globally a p-th power,

(b) The class number of L is prime to p (or equivalently, the mapping $\oplus_{v\in S}\bar{E}_v\to\bar{P}$ is surjective), and

(c) The mapping $\mu_p(L)\to\oplus_{v\in S}\mu_p(L_v)$ is surjective (and hence is an isomorphism).

Remark. If conditions (a) and (b) hold (e.g., if (L, S) is neat for p) then the sequence

$$0\longrightarrow\bar{E}\longrightarrow\oplus_{v\in S}\bar{E}_v\longrightarrow\bar{P}\longrightarrow 0 \tag{1.3}$$

is exact.

For the remainder of this section we suppose that *the pair* (L, S) *is neat for* p, *and the cardinality of* A *is prime to* p.

Let $C\subset A$ denote the subgroup generated by the image of a complex conjugation involution (so that C is either trivial or of order 2, according to whether L is totally real or totally complex). In the statement and proof of the proposition below, we shall refer to the following $\boldsymbol{F}_p[A]$-modules: $\boldsymbol{F}_p$ (given trivial A-action), $\mu_p(L)$ and $\mu_p(L_v)$ (given their natural Galois actions), $\mathrm{Ind}_C^A\boldsymbol{F}_p$ (the $\boldsymbol{F}_p[A]$-module obtained by inducing the trivial $\boldsymbol{F}_p[C]$-module $\boldsymbol{F}_p$ to A), and $\boldsymbol{F}_p[A]$ (the free module of rank 1).

Proposition 2. *We have isomorphisms of* $\boldsymbol{F}_p[A]$*-modules*

$$\bar{P}\oplus\mathrm{Ind}_C^A\boldsymbol{F}_p\cong\boldsymbol{F}_p[A]\oplus\boldsymbol{F}_p.$$

Proof. We use the exact sequence (1.3) of $\boldsymbol{F}_p[A]$-modules and compute the $\boldsymbol{F}_p[A]$-module structure of the first two nonzero terms in (i) and (ii) below. The proposition then follows.

$$\bar{E}\oplus\boldsymbol{F}_p\cong\mathrm{Ind}_C^A\boldsymbol{F}_p\oplus\mu_p(L) \tag{i}$$

(*Proof.* The fact that the representation of $\boldsymbol{Q}[A]$ on $\boldsymbol{Q}\otimes(E\oplus\boldsymbol{Z})$ is isomorphic to the permutation representation of A on cosets mod C is due originally to Herbrand. Here the A-action on $\boldsymbol{Z}$ is meant to be the trivial action. See [T] I §4 for a proof of Herbrand's theorem and for historical discussion. Statement (i) can then be obtained from this as an easy exercise, using that the cardinality of A is prime to p.)

$$\oplus_{v\in S}\bar{E}_v\cong\boldsymbol{F}_p[A]\oplus\{\oplus_{v\in S}\mu_p(L_v)\}. \tag{ii}$$

(*Proof.* Use the p-adic logarithm to induce an A-equivariant isomorphism between an open subgroup of finite index in the p-adic Lie group $\oplus_{v\in S}E_v$ and $\mathcal{O}_L\otimes\boldsymbol{Z}_p$. Then an easy exercise, similar to the one for (i), gives the assertion.)

If L is totally complex, i.e., if C is of order 2, let $\tilde{\boldsymbol{F}}_p$ denote the one-dimensional $\boldsymbol{F}_p[C]$-representation with nontrivial C-action. Then:

Corollary 1. *If L is totally real, we have*

$$\bar{P}\cong\boldsymbol{F}_p,$$

while if L is totally complex, we have

$$\bar{P}\cong\mathrm{Ind}_C^A\tilde{\boldsymbol{F}}_p\oplus\boldsymbol{F}_p.$$

1.3. Generators and relations for P_p and P

If H is any pro-p-group, then its generator and relation ranks (cf. [K], § 6) will be denoted $d(H)$ and $r(H)$ respectively.

If F is a field, let $\delta(F)=1$ if F contains a nontrivial p-th root of 1, $\delta(F)=0$ otherwise.

Proposition 3 [K] Sätze 10.3, 10.5.
(a) $r(P_p)=\delta(L_p)$
(b) $d(P_p)=[L_p\colon\boldsymbol{Q}_p]+1+\delta(L_p)$.

Let r_2 be the number of complex places of L. Let $W\subset L^*$ denote the subgroup of elements $x\in L^*$ satisfying the condition that the fractional ideal (x) is a p-th power and the image of x in L_v^* is a p-th power for all $v\in S$. Then W contains L^{*p}. Put $B:=W/L^{*p}$, viewed as an $\boldsymbol{F}_p$-vector space. Note that if (L, S) is neat for p, then $B=0$.

Proposition 4 [K] Satz 11.8, [N].
(a) $r(P)=(\sum_{v\in S}\delta(L_v))-\delta(L)+\dim B$
(b) $d(P)=r_2+1+r(P)$.

Corollary 2. *P is a free pro-p-group if and only if*
(i) $B=0$
(ii) *the mapping $\mu_p(L)\to\oplus_{v\in S}\mu_p(L_v)$ is surjective.*

Corollary 3. *If (L, S) is neat for p, then P is a free pro-p-group.*

Remark. Parts (b) of Propositions 3 and 4 also follow from Propositions 1 and 2 of § 1.2, respectively.

Chapter 2. The Particular Set-up

Let K/Q be a cubic field extension satisfying these properties:
(a) The field K is not totally real, and
(b) The rational prime p splits in the ring of integers of K as follows:

$$(p)=\mathscr{P}_1\cdot\mathscr{P}_2$$

where $\mathscr{P}_1$ is of degree 1, and $\mathscr{P}_2$ is ramified, of ramification index 2. We may view K as a subfield of $\boldsymbol{Q}_p$ by completing K with respect to $\mathscr{P}_1$.

Either of the two properties (a), (b) insure that K is nonGalois over $\boldsymbol{Q}$. Let $L/\boldsymbol{Q}$ denote the Galois closure of K in $\bar{\boldsymbol{Q}}$, and let v_1, v_2, v_3 denote the three places of L above, p, where v_1 is the unique place lying above the prime p_1 of K, i.e., $L_{v_1}=L_p$ and the decomposition group at v_1 is G_p. Let $\sigma\in\mathrm{Gal}(L/\boldsymbol{Q})$ denote the involution fixing K (equivalently: fixing v_1) and let $\tau\in\mathrm{Gal}(L/\boldsymbol{Q})$ denote the element of order 3 which cyclically permutes v_1, v_2, v_3 (τ: $v_1\mapsto v_2$, etc.).

Definition 3. A cubic field extension $K/\boldsymbol{Q}$ is admissible if it satisfies (a), (b) above, and if in addition (L, S) is neat for p, where $S=\{v_1, v_2, v_3\}$.

Examples. Recall the notion of *special* S_3*-extension* [M]: For prime numbers p of the form $p=27+4a^3$ with $a\in\boldsymbol{Z}$, let K be the cubic field $\boldsymbol{Q}(x)$ where x is a root of x^3+ax+1. We refer to K as a *special cubic field* (of discriminant $-p$); its Galois closure $L/\boldsymbol{Q}$ is called a *special* S_3*-extension.* It is shown in [M] that special cubic fields are admissible. The primes $p<1{,}000{,}000$ of the form $27+4a^3$ are: 23, 31, 59, 283, 1399, 4027, 5351, 11003, 16411, 32,027, 97,583, 119,191, 157,243, 202,639, 275,711, 415,319, 562,459, and 665,527.

Now *fix an admissible cubic extension* $K/\boldsymbol{Q}$, and let $A:=\mathrm{Gal}(L/Q)$ denote the Galois group, isomorphic to the symmetric group on three letters, with generators σ, τ as described above. Let $A_p:=\{1, \sigma\}\subseteq A$. Let $\bar{\rho}$: $\mathrm{Gal}(L/\boldsymbol{Q})\hookrightarrow GL_2(\boldsymbol{F}_p)$ be a choice of imbedding, and denote by the same letter the homomorphism from $G_{\boldsymbol{Q}}$ to $GL_2(\boldsymbol{F}_p)$ obtained by composition with the natural projection $G_{\boldsymbol{Q}}\twoheadrightarrow\mathrm{Gal}(L/\boldsymbol{Q})$. As above, let G denote the p-completion of $G_{\boldsymbol{Q}}$ relative to $\bar{\rho}$ and S. Then $\bar{\rho}$ factors through G to give a continuous homomorphism (denoted by the same letter)

$$\bar{\rho}\colon G\longrightarrow GL_2(\boldsymbol{F}_p).$$

Let E denote the group of global units in L, and E_i ($i=1, 2, 3$) denote the groups of local units in the completions L_i of L with respect to the places v_i ($i=1, 2, 3$). Let

$$\begin{tikzcd}
1 \arrow[r] & P \arrow[r] & G \arrow[r] & A \arrow[r] & 1 \\
1 \arrow[r] & P_p \arrow[r] \arrow[u] & G_p \arrow[r] \arrow[u] & A_p \arrow[r] \arrow[u] & 1
\end{tikzcd} \tag{2.1}$$

be the diagram (1.2) of § 1.1 coming from our fixed admissible cubic extension $K/\boldsymbol{Q}$, with $S=\{v_1, v_2, v_3\}$.

Let

$$0 \longrightarrow \bar{E} \longrightarrow \bar{E}_1 \oplus \bar{E}_2 \oplus \bar{E}_3 \longrightarrow \bar{P} \longrightarrow 0 \tag{2.2}$$

be the exact sequence of p-Frattini quotients (1.3) of §1.2, which we view as $\boldsymbol{F}_p[A]$-modules. By our conventions, the image of $\bar{E}_1$ in $\bar{P}$ is equal to the image of $\bar{P}_p^0$ in $\bar{P}$.

2.1. The action of A on the p-Frattini quotients

We now *suppose that p is greater than* 3. Up to equivalence, there are three irreducible representations of A over the field $\boldsymbol{F}_p$:

$1=$the trivial representation

$\varepsilon=$the sign representation

$\chi=$the irreducible 2-dimensional representation.

Proposition 5. *There is an F_p-basis of $\bar{P}_p$ consisting of three elements $\bar{\xi}$, $\bar{\eta}$, $\bar{\varphi}$ such that $\bar{\xi}$ and $\bar{\eta}$ generate $\bar{P}_p^0$ and the action of the involution σ in A_p is given by the rule*: $\sigma(\bar{\xi})=\bar{\xi}$; $\sigma(\bar{\eta})=-\bar{\eta}$; $\sigma(\bar{\varphi})=\bar{\varphi}$.

Proof. This is just Proposition 1 applied to our particular set-up.

Proposition 6. *The p-Frattini quotient $\bar{P}$ is* 4*-dimensional. The natural action of A on $\bar{P}$ is equivalent to* $1\oplus\varepsilon\oplus\chi$.

Proof. This is just Proposition 2 applied to our particular set-up.

2.2. Generators and relations

The pro-p group P is free by Corollary 3 in § 1.3; the pro-p-group P_p is free by Proposition 3 of § 1.3. The group G is a semi-direct product of A by P via an action of A on P which is uniquely determined up to (noncanonical) isomorphism by the isomorphism class of the A module $\bar{P}$ (see [B]).

Proposition 7. *Let Π be the free pro-p group on* 4 *generators labelled u, $\tau(u)$, $\tau^2(u)$, v. Define an A-action on Π by the following prescription*:

(a) *$\tau(v)=v$, and τ cyclically permutes the three generators u, $\tau(u)$, $\tau^2(u)$ in the evident manner.*

(b) *$\sigma(u)=u$ and $\sigma(v)=v^{-1}$.*

Let $A \ltimes \Pi$ denote the semi-direct product of Π by A, with the above action of A on Π.

Then there are isomorphisms as indicated, making the diagram below commutative:

$$\begin{tikzcd}
1 \arrow[r] & \Pi \arrow[r] \arrow[d, "\cong"', "i"] & A \ltimes \Pi \arrow[r] \arrow[d, "\cong"', "i"] & A \arrow[r] \arrow[d, "="', "\text{(identity)}"] & 1 \\
1 \arrow[r] & P \arrow[r] & G \arrow[r] & A \arrow[r] & 1
\end{tikzcd}$$

Proof. The prescription (a), (b) extends to an A-action on Π as is easily seen. This A-action induces an A-module structure on the p-Frattini quotient group $\bar{\Pi}$ which is equivalent to the A-module structure of $\bar{P}$. The proposition then follows from [B] Proposition 2.7.

How much freedom do we have in choosing the isomorphism i? A partial answer is given by the following

Addendum (to Proposition 7). Choose an A-action on P that lifts the natural A-action on $\bar{P}$. Let $\circ$ denote this A-action. Let $w \in P$ be any element such that $\sigma \circ w=w$, and the three elements

$$\bar{w}, \quad \tau \circ \bar{w}, \quad \tau^2 \circ \bar{w}$$

are linearly independent in $\bar{P}$. Then there is an isomorphism i as in Proposition 7 such that

(i) for all $a \in A$ and $z \in P$, $a \circ z$ is the conjugate of z by $i(a)$,

(ii) $i(u)=w$.

Proof. Let a complement in $\bar{P}$ of $\langle \bar{w}, \tau \circ \bar{w}, \tau^2 \circ \bar{w} \rangle$ (as $F_p[A]$-modules) be generated by $\bar{t}$. Then $\sigma \circ \bar{t}=\bar{t}^{-1}$, $\tau \circ \bar{t}=\bar{t}$.

By [B], Theorem 2.8, there exists $t \in P$ mapping to $\bar{t}$ with $\sigma \circ t=t^{-1}$, $\tau \circ t=t$. Define a mapping $i\colon \Pi \to P$ by setting $i(u)=w$, $i(v)=t$ and insisting (as is possible because of the compatibility of A-actions) that i commute with the action of A. The homomorphism i extends to a homomorphism $A \ltimes \Pi \to A \ltimes P$ (setting i to be the identity on A) and it is an isomorphism since there is the obvious inverse j defined by $j(w)=u, j(t)=v$. (By Burnside's lemma, P is generated by w, $\tau \circ w$, $\tau^2 \circ w$, t.)

Proposition 8. *Let Π_p be the free pro-p group on 3 generators labelled ξ, η, φ. Define an action of the cyclic group $A_p=\{1, \sigma\}$ on Π_p by letting σ fix ξ and φ and $\sigma(\eta)=\eta^{-1}$. Then there is a commutative diagram where the* *vertical maps are isomorphisms*:

$$\begin{tikzcd}
1 \arrow[r] & \Pi_p \arrow[r] \arrow[d, "\cong"', "i"] & A_p \ltimes \Pi_p \arrow[r] \arrow[d, "\cong"', "i"] & A_p \arrow[r] \arrow[d, "="'] & 1 \\
1 \arrow[r] & P_p \arrow[r] & G_p \arrow[r] & A_p \arrow[r] & 1
\end{tikzcd}$$

and where the semi-direct product is with the action described above. Moreover, the generators ξ, η *of* Π_p *are mapped, under the vertical isomorphism, to the image of the inertia group.*

Proof. The given A_p-action on Π_p induces an A_p-module structure on the p-Frattini quotient group $\bar{\Pi}_p$ which is equivalent to the A_p-module structure of $\bar{P}_p$. The first part of the Proposition follows then from [B] Proposition 2.7. The second part follows similarly, using Proposition 5 and [B] Proposition 2.7.

Remark. So far we have not made any connection between the presentation of G_p and the presentation of G.

2.3. Generic vs. degenerate cases

Returning to the exact sequence (2.2) of $F_p[A]$-modules, let $\bar{P}_i \subset \bar{P}$ denote the image of $\bar{E}_i$ for $i=1, 2, 3$. Thus $\bar{P}_1$ is the image of $\bar{P}_p^0$ in $\bar{P}$. Denote by d the dimension (over F_p) of the image of the projection mapping

$$\bar{E} \xrightarrow{\Pi_i} \bar{E}_i.$$

Since the projections Π_i $(i=1, 2, 3)$ are permuted transitively under the action of A, this dimension is independent of i. Note that, by exactness of (5), d is greater than 0. We therefore have only two possible cases:

(I) **The generic case:** $d=2$

If $d=2$, i.e., *the projections are isomorphisms, then the images* $\bar{P}_i$ *are pairwise transversal,* i.e., $\bar{P}_i \cap \bar{P}_j = 0$ for $i \neq j$. To see this, just note that if there were elements $y_i \in \bar{E}_i$, $y_j \in \bar{E}_j$ such that the image of y_i in $\bar{P}_i$ were equal to the image of $-y_j$ in $\bar{P}_j$, then the element $y_i \oplus y_j \oplus 0 \in \bar{E}_i \times \bar{E}_j \times \bar{E}_k$ would be in the image of $\bar{E}$, i.e., there would be an element $y \in \bar{E}$ such that $\Pi_i(y)=y_i$, $\Pi_j(y)=y_j$, and $\Pi_k(y)=0$. But Π_k is an isomorphism, giving that $y_i=y_j=0$. Here k is the index such that $\{i, j, k\}=\{1, 2, 3\}$.

(II) **The degenerate case:** $d=1$

If $d=1$, *the intersection* $\bar{P}_1 \cap \bar{P}_2 \cap \bar{P}_3$ is a 1-*dimensional* F_p *vector space.* To see this, first note that the image $\Pi_1(\bar{E}) \subset \bar{E}_1$ is a 1-dimensional vector space, stable under the action of $\sigma=\sigma_1$, the involution in A which fixes v_1.

There are only two such subspaces, the + or − eigenspace for the action of σ. Let $\varepsilon=\pm 1$ corresponding to the sign of the eigenvalue of σ on this image. It then follows, by symmetry, that the image $\Pi_i(\bar{E})\subset\bar{E}_i$ is equal to the ε-eigenspace for the action of σ_i, the involution in A which fixes v_i $(i=1, 2, 3)$. Now take an element $e\neq 0$ in $\bar{E}$ which is in the kernel of σ_1. Let $e_i=\Pi_i(e)$ for $i=1, 2, 3$. Then $0\oplus e_2\oplus e_3$ maps to zero in $\bar{P}$. Since e_2 and e_3 cannot both be zero (exactness of (2.2)) neither can be zero. Their images in $\bar{P}$ generate the *same* 1-dimensional F_p-vector space. By construction, e_i (for $i=2$ or 3) is in the image of $\bar{E}$ under Π_i. Therefore e_i generates the ε-eigenspace in $\bar{E}_i$ for the involution σ_i. It therefore follows that the ε-eigenspaces for the involutions σ_i acting on the subspace $\bar{P}_i\subset\bar{P}$ coincide, for $i=2, 3$. Now, it cannot be the case that $\bar{P}_2$ coincides with $\bar{P}_3$. For then, by symmetry, all three subspaces $\bar{P}_j$ $(j=1, 2, 3)$ would coincide, contradicting the fact that they generate $\bar{P}$. It follows that $\bar{P}_2\cap\bar{P}_3$ is equal to the 1-dimensional space which can be described, alternatively, as the ε-eigenspace for the involution σ_2 in $\bar{P}_2$ or the ε-eigenspace for the involution σ_3 in $\bar{P}_3$. By symmetry, it is *also* the ε-eigenspace for the involution $\sigma_1=\sigma$ in $\bar{P}_1$, establishing our claim.

To justify the terminology "generic" and "degenerate" we shall give a necessary and sufficient numerical condition for a special S_3-extension to be generic, and show that there are indeed lots of them. Let, then, as in §4 and [M], p be of the form $27+4a^3$ for $a\in \boldsymbol{Z}$, and suppose that $K=\boldsymbol{Q}(x)$ is the cubic field generated by the element x which is a root of x^3+ax+1. As above, let $L/\boldsymbol{Q}$ be the Galois closure of $\boldsymbol{Q}$.

Proposition 9. *$L/\boldsymbol{Q}$ is a degenerate S_3-extension if and only if*

$$\frac{1-(a/3)^{p-1}}{p}\equiv 4/3^5 \qquad \text{mod } p, \tag{2.3}$$

the equation being a congruence of p-units (say in $\boldsymbol{Z}_p$).

Proof. Denote by x_1 the unique root of x^3+ax+1 in $\boldsymbol{Q}_p$, and let x_2, x_3 denote the two other quadratic conjugate roots in $\bar{\boldsymbol{Q}}_p$. Write:

$$x_1\equiv(3+c\cdot p)/a \qquad \text{mod } p^2 \tag{2.4}$$

and solve for c mod p, giving $c\equiv 1/(27+a^3)$ mod p.

Now define p-adic integers B, C by the factorization

$$X^3+aX+1=(X-x_1)(X^2+BX+C)$$

giving $B=x_1$ and $C=a+x_1^2$. The roots x_2, x_3 are then roots of X^2+BX+C.

Lemma 1. *Let $F/\mathbf{Q}_p$ be the splitting field of X^2+BX+C. Then x_2/x_3 is not a p-th power in F.*

Proof. Put $D=B^2-4C$ so that $D=-3x_1^2-4a$. Using the determination of x_1 mod p^2 given above, one obtains

$$D\equiv\left(\frac{-1}{x_1(2+a^3)}\right)\cdot p \qquad \bmod p^2.$$

The p-adic integer D is a square in F, and since $p\neq 2$ and the expression in the large parenthesis above is a p-adic unit, there is a uniformizer π in the ring of integers of F such that $\pi^2=D/4$ and $x_2=-x_1/2+\pi$, $x_3=-x_1/2-\pi$. To prove the lemma, we show that

$$x_2^{p-1}\not\equiv x_3^{p-1} \bmod \pi^2$$

or equivalently,

$$x_2^p x_3\not\equiv x_3^p x_2 \bmod \pi^2.$$

But $x_2^p\equiv x_3^p\equiv(-x_1/2)^p$ mod π^2, and, since $2\pi\not\equiv 0$ mod π^2, we have that $x_2\not\equiv x_3$ mod π^2. The displayed noncongruence above then follows, as does our lemma.

Lemma 2. *The — eigenspace for the involution σ_i in $\bar{E}_i$ is in the image of Π_i: $\bar{E}\rightarrow\bar{E}_i$ $(i=1, 2, 3)$.*

Proof. It suffices to prove Lemma 2 for $i=1$. But x_2/x_3 is in the — eigenspace of σ_1 in $\bar{E}$. It is visibly in the image of $\bar{E}$. By Lemma 1, it projects nontrivially to $\bar{E}_1$.

Lemma 3. *The + eigenspace for the involution σ_i in $\bar{E}$ is in the kernel of Π_i (for all or equivalently for any $i=1, 2, 3$) if and only if the congrence* (2.3) *holds.*

Proof. Again it suffices to prove our lemma for $i=1$. The element $x\in K$ is in E, and its image in $\bar{E}$ generates the + eigenspace for σ. It follows that the + eigenspace for σ in $\bar{E}$ projects to zero under Π_1 if and only if x_1 is a p-th power in $\mathbf{Q}_p$. But x_1 is a p-th power if and only if $x_1^{p-1}\equiv 1 \bmod p^2$. A simple computation using the congruence (2.4) mod p^2 together with the determination of c establishes that $x_1^{p-1}\equiv 1 \bmod p^2$ if and only if the congruence (2.3) holds.

From Lemmas 2 and 3 we see that Π_i: $\bar{E}\rightarrow\bar{E}_i$ is an isomorphism if and only if congruence (2.3) doesn't hold, whence our proposition.

Computation. We verified that the congruence (2.3) does *not* hold for all primes $p<11{,}003$ in the list given in Chapter 2. Thus for all special S_3-extensions corresponding to these prime numbers we are in the "generic" case. We have no example of a "degenerate" case.

2.4. Linking local and global presentations

We identify G with $A \ltimes \Pi$ and G_p with $A_p \ltimes \Pi_p$ as in Propositions 7 and 8 of Section 2.2. Thus, the pro-p group has, as system of generators: u, $\tau(u)$, $\tau^2(u)$, v. The pro-p group Π_p has, as system of generators: x, y, z.

The mapping $G_p \rightarrow G$ restricts to a mapping of Π_p into Π.

Proposition 10. *If the admissible cubic extension $K/\boldsymbol{Q}$ has Galois closure $L/\boldsymbol{Q}$ which is generic, then we may take the local and global system of generators so that under the mapping $\Pi_p \rightarrow \Pi$, the image of ξ is u, and if $^-$ denotes projection to p-Frattini quotient groups the image of $\bar\eta$ is $\bar v+2(\tau(\bar u)-\tau^2(\bar u))$.*

Proof. Under the identification $\Pi \cong P$, let $\bar\Pi_i$ correspond to the image of the i-th inertia group $\bar P_i$ in $\bar\Pi$, for $i=1, 2, 3$. Recall that, as A-module, $\bar\Pi$ is isomorphic to $1 \oplus \varepsilon \oplus \chi$. Let r, s denote the images of the generators $x, y \in \Pi_p$. Let $\bar R$, $\bar S \subset \bar\Pi$ denote the A-stable subspaces generated by $\bar r$, $\bar s$ respectively.

Lemma 4. *As A-modules, $\bar R \cong 1 \oplus \chi$ and $\bar S \cong \varepsilon \oplus \chi$.*

Proof. First we note that neither $\bar R$ nor $\bar S$ can be 1-dimensional over $\boldsymbol{F}_p$. For, if they were, they would be contained in $\bar\Pi_1$ (since they would be generated by $\bar r$ or $\bar s$, respectively) and hence by symmetry they would be in the intersection of $\bar\Pi_i$ for $i=1, 2, 3$ which is impossible, by our genericity assumption. Also note that, by construction, $\bar R$ is a quotient of the induced A-module $\mathrm{Ind}^A_{A_p}(1)$ and $\bar S$ is a quotient of $\mathrm{Ind}^A_{A_p}(\varepsilon)$.

Since $\mathrm{Ind}^A_{A_p}(1)=1\oplus\chi$, and $\mathrm{Ind}^A_{A_p}(\varepsilon)=\varepsilon\oplus\chi$, and since $\bar R+\bar S=\bar\Pi$ the lemma follows.

From the lemma it follows that the elements $\bar r$, $\tau(\bar r)$, $\tau^2(\bar r)$ are linearly independent in $\bar\Pi$, and, of course, $\sigma(\bar r)=\bar r$. From the addendum to Proposition 7 of Section 2.2, it follows that we may take u to be image of ξ, and complete u, $\tau(u)$, $\tau^2(u)$ to a basis as in Proposition 7, by the appropriate choice of v.

Since $\sigma(\bar\eta)=-\bar\eta$, it follows that $\bar s=a\cdot\bar v+b(\tau(\bar u)-\tau^2(\bar u))$ for appropriate choice of $a, b \in \boldsymbol{F}_p$. From the lemma it follows that neither a nor b is zero. By appropriate modification of the choice of ξ (hence of u), and v (replacing them by appropriate powers of themselves) we may arrange it so that $a=1$ and $b=2$.

Chapter 3. Universal Deformations

3.1. The explicit description

Let $K/\boldsymbol{Q}$ be an admissible cubic extension, which can be either generic or degenerate. We keep to the notation of Chapter 2. In particular, we have the continuous homomorphism

$$\bar{\rho}\colon G \longrightarrow GL_2(F_p)$$

given in Chapter 2.

Let $\mathscr{A}$ be a complete noetherian local ring with residue field $\boldsymbol{F}_p$. Two liftings ρ_0 and ρ_0' of $\bar{\rho}$ are *strictly equivalent* if ρ_0' can be brought to ρ_0 by conjugation

(3.1)
$$\begin{tikzcd}
 & GL_2(\mathscr{A}) \arrow[dd] \\
G \arrow[ur, shift left, "{\rho_0, \rho_0'}"] \arrow[ur, shift right] \arrow[dr, "\bar{\rho}"'] & \\
 & GL_2(\boldsymbol{F}_p)
\end{tikzcd}$$

by an element in the kernel of the projection of $GL_2(\mathscr{A})$ to $GL_2(\boldsymbol{F}_p)$. A *deformation* of $\bar{\rho}$ to $\mathscr{A}$ is a strict equivalence class of liftings of $\bar{\rho}$ to $\mathscr{A}$. It is shown in [M] (see also [B]) that *a universal deformation* of $\bar{\rho}$ exists. Let R denote the universal deformation ring of $\bar{\rho}$, and

$$\rho\colon G \longrightarrow GL_2(R)$$

the universal deformation (or more accurately: a representative lifting in its strict equivalence class). We *identify* G with $A \ltimes \Pi$ and P with Π as in Proposition 7.

Proposition 11. *We may identify R with the power series ring in* 3 *variables $\boldsymbol{Z}_p[[T_1, T_2, T_3]]$ and we may give the following description of the universal deformation ρ:*

(i) $\sigma \mapsto \begin{pmatrix} +1 & 0 \\ 0 & -1 \end{pmatrix}$

(ii) $\tau \mapsto \begin{pmatrix} -1/2 & 1/2 \\ -3/2 & -1/2 \end{pmatrix}$

(iii) $u \mapsto \begin{pmatrix} 1+T_1 & 0 \\ 0 & 1+T_2 \end{pmatrix}$.

(iv) $v \mapsto \begin{pmatrix} (1-3T_3^2)^{1/2} & T_3 \\ -3T_3 & (1-3T_3^2)^{1/2} \end{pmatrix}$

Proof. Consider any deformation ρ of $\bar{\rho}$ to a complete local noetherian ring $\mathscr{A}$, with residue field $\boldsymbol{F}_p$. That is, we are given a strict equivalence class of liftings

$$\begin{tikzcd} A \ltimes \Pi \arrow[r, "\rho_0"] \arrow[d] & GL_2(\mathscr{A}) \arrow[d] \\ A \arrow[r, "\bar{\rho}"] & GL_2(\boldsymbol{F}_p) \end{tikzcd}$$

The ring $\mathscr{A}$ has a unique $\boldsymbol{Z}_p$-algebra structure, and there is a *unique* representative lifting whose restriction to $A \subset A \ltimes \Pi$ is prescribed by the formula (i) and (ii) in the statement of our proposition, composed with the natural homomorphism $GL_2(\boldsymbol{Z}_p) \to GL_2(\mathscr{A})$ induced by the $\boldsymbol{Z}_p$-algebra structure of $\mathscr{A}$. Let ρ refer to this unique representative lifting. By Proposition 7 (b) it follows that $\rho(u)$ is a diagonal matrix in the kernel of reduction to $GL_2(\boldsymbol{F}_p)$. As for $\rho(v)$, it too is in the kernel of reduction to $GL_2(\boldsymbol{F}_p)$. From Proposition 7 (a) one sees that $\rho(v)$ is a matrix of the form

$$\begin{pmatrix} a & b \\ -3b & a \end{pmatrix}$$

for elements $a \equiv 1 \bmod \mathfrak{m}_{\mathscr{A}}$ and $b \in \mathfrak{m}_{\mathscr{A}}$, where $\mathfrak{m}_{\mathscr{A}}$ is the maximal ideal of $\mathscr{A}$. From Proposition 7 (b) one also has that $\rho(v)$ is of determinant 1.

It follows that there are elements $t_1, t_2, t_3 \in \mathfrak{m}_{\mathscr{A}}$ such that

$$\rho(u) = \begin{pmatrix} 1+t_1 & 0 \\ 0 & 1+t_2 \end{pmatrix}; \qquad \rho(v) = \begin{pmatrix} (1-3t_3^2)^{1/2} & t_3 \\ -3t_3 & (1-3t_3^2)^{1/2} \end{pmatrix}.$$

Our proposition follows immediately from this.

3.2. The generic case

From now on we make the assumption that the Galois closure $L/\boldsymbol{Q}$ of our admissible cubic extension $K/\boldsymbol{Q}$ is *generic*. We also suppose that we have chosen a system of generators for G_p and for G which are *linked* in the sense of Proposition 10 of Section 2.4.

Proposition 12. *Let* $\mathfrak{m}$ *be the maximal ideal of* $\boldsymbol{Z}_p[[T_1, T_2, T_3]]$. *There are power series* $f, g \in \mathfrak{m}$ *such that*

(i) $f(T_1, T_2, T_3) = T_1 - T_2 + T_3 \quad \bmod \mathfrak{m}^2$
$g(T_1, T_2, T_3) = 3T_1 - 3T_2 - 3T_3 \quad \bmod \mathfrak{m}^2$

and such that

(ii) $\rho(\eta)=\begin{pmatrix}(1+fg)^{1/2} & f \\ g & (1+fg)^{1/2}\end{pmatrix}$

Proof. The existence of power series f, g satisfying (ii) is immediate from the fact that $\sigma(\eta)=\eta^{-1}$ (which gives that $\rho(\eta)$ has determinant 1, and diagonal entries equal).

To verify (i), first note that since the kernel of the natural projection

$$GL_2(\boldsymbol{Z}_p[[T_1, T_2, T_3]]/\mathfrak{m}^2) \twoheadrightarrow GL_2(\boldsymbol{F}_p)$$

is an elementary p-abelian group, the homomorphism

$$\rho\colon P \longrightarrow GL_2(\boldsymbol{Z}_p[[T_1, T_2, T_3]])$$

induces a homomorphism

$$\bar{P} \longrightarrow GL_2(\boldsymbol{Z}_p[[T_1, T_2, T_3]]/\mathfrak{m}^2).$$

By Proposition 10 we have that the image of $\bar{\eta}$ under the natural mapping $\bar{\Pi}_p \to \bar{\Pi}$ is $\bar{v}+2(\tau(\bar{u})-\tau^2(\bar{u}))$ and by Proposition 11 we have the explicit description of $\rho(v)$ and $\rho(u)$. A simple computation then gives (i).

3.3. Fine structure of the universal deformation space

Let $X=\mathrm{Hom}_{\mathrm{cont}}(\boldsymbol{Z}_p[[T_1, T_2, T_3]], \boldsymbol{Z}_p)$ which we view as a 3-dimensional analytic manifold (over $\boldsymbol{Q}_p$). We make the identification

$$X \cong p\boldsymbol{Z}_p \times p\boldsymbol{Z}_p \times p\boldsymbol{Z}_p$$

by associating to $x \in X$ the triple $(x(T_1), x(T_2), x(T_3))$. To each $x \in X$ we have the image of the representation ρ under x, which we denote

$$\rho_x\colon G \longrightarrow GL_2(\boldsymbol{Z}_p).$$

In [M] a glossary of properties of representations ρ_x was given ([M] Chap. II § 1). In the definition below we recall some of these properties, giving somewhat briefer definitions, which are nevertheless equivalent to the definitions given in [M] in the special context of the present paper.

Definition 4. The point $x \in X$ is called

(a) *inertially reducible* if the image of an inertia subgroup at p under ρ_x is contained in a Borel subgroup of $GL_2(\boldsymbol{Q}_p)$.

(b) *globally* (resp. *inertially*) *dihedral* if the image of G (resp. an inertia subgroup at p) under ρ_x is contained in the normalizer of a Cartan subgroup of $GL_2(\boldsymbol{Q}_p)$.

(c) *ordinary* if an inertial subgroup at p, acting via ρ_x, has a nontrivial fixed vecter, and

(d) *inertially ample* if the Lie algebra of the image of an inertia subgroup at p under ρ_x contains $\mathfrak{sl}_2(\boldsymbol{Q}_p)$.

In [M] information was given concerning the locus in the universal deformation space of any special dihedral representation of points x satisfying each of the properties listed above. In the context of this article (i.e., for generic S_3-representations) we can give a complete explicit description of each of these loci:

Proposition 13. (a) *The inertially reducible locus consists in the union of the two smooth* (*hyper*) *surfaces in* X *defined by the equations* $f=0$ *and* $g=0$.

(b) *The globally dihedral locus in* X *is equal to the inertially dihedral locus and consists in the smooth* (*hyper*) *surface defined by the equation*

$$T_1=T_2.$$

(c) *The ordinary locus in* X *consists in the smooth analytic curve defined by the simultaneous equations*

$$g=0$$
$$T_1=0.$$

(d) *The inertially ample locus in* X *is given by the complement of the three* (*hyper*) *surfaces*

$$f=0, \quad g=0, \quad \textit{and} \quad T_1=T_2.$$

Proof. We begin with a "transversality" lemma:

Lemma 5. *The following pairs of power series are transversal, i..e., their images in* $\mathfrak{m}/\mathfrak{m}^2$ *are linearly independent over* $\boldsymbol{F}_p$:

(i) f *and* g
(ii) g *and* T_1
(iii) f *and* T_1
(iv) f *and* T_1-T_2
(v) g *and* T_1-T_2.

Proof. Immediate from Proposition 12 (i).

Note in particular that $f=0$ and $g=0$ are the equations of smooth hypersurfaces in X.

Lemma 6. *If $g(x)=0$ (resp., $f(x)=0$) then the image of the decomposition group G_p under ρ_x lies in the subgroup of upper (resp., lower) triangular matrices.*

Proof. If $g(x)=0$, then the generator η is visibly sent to an upper triangular matrix. But the generators ξ and ϕ are sent to diagonal matrices. With an identical argument if $f(x)=0$, our lemma follows.

Lemma 7. *If x is inertially reducible, then the image of inertia at p under ρ_x is contained in either the subgroup of upper or lower triangular matrices.*

Proof. The involution σ is sent to $\begin{pmatrix} +1 & 0 \\ 0 & -1 \end{pmatrix}$ and normalizes the image of the inertia subgroup.

Proof of (a). By Lemma 2 the hypersurfaces $f=0$ and $g=0$ comprise inertially reducible points. By Lemma 3 any inertially reducible point x must have either $f(x)=0$ or $g(x)=0$.

Lemma 8. *If x is inertially dihedral, then x lies on the hyperplane $T_1=T_2$, or else it lies on the smooth curve $f=g=0$.*

Proof. If x is inertially dihedral, then the image of the generators ξ and η under ρ_x must commute. This gives us the equations:

$$g(x)(t_1-t_2)=0 \quad \text{and} \quad f(x)(t_1-t_2)=0.$$

Lemma 9. *If $t_1=t_2$, then x is globally dihedral.*

Proof. Under the above hypothesis, $\rho(u)$ is a scalar, hence so is $\rho(\tau(u))$ and $\rho(\tau^2(u))$. These matrices must commute with $\rho(v)$, and therefore the image of Π is abelian, and is centralized by τ.

Proof of (b). We first show that the smooth curve

$$C: f=g=0$$

actually lies in the hyperplane $T_1=T_2=0$. *Suppose not.* Note that (Lemma 6) the points of C are inertially dihedral. Next, note that twisting by wild 1-dimensional characters ([M] Chap. I Section 2 (6.2)) preserves the inertially dihedral locus. It follows, under our assumption, that the curve C is preserved by such twisting as is the hyperplane $T_1-T_2=0$. But C and $T_1-T_2=0$ have a nontrivial intersection. The orbit of this intersection under twisting generates C and lies on the hyperplane $T_1-T_2=0$, establishing our claim.

Assertion (b) then follows from Lemmas 8 and 9.

Proof of (c). One easily sees (compare Lemma 7) that if x is ordinary, then the image of inertia under ρ_x is contained in the subgroup of upper triangular matrices, and $t_1=0$. The converse statement is immediate.

Proof of (d). Given that the image of $\bar{\rho}$ is isomorphic to S_3 there are only three possibilities: x is inertially reducible, inertially dihedral, or ample. Assertion (d) then follows from (a) and (b).

Remark. Let $R^0 := \boldsymbol{Z}_p[[T_1, T_2, T_3]]/(g, T_1)$, which by (c) we have shown to be the universal ordinary deformation ring for $\bar{\rho}$ ([M] Chap. II § 5). The determinant mapping ([M] Chap. II, § 4)

$$\Lambda \overset{\gamma}{\cong} \boldsymbol{Z}_p[[T]] \xrightarrow{\delta} R^0$$

may be taken to be $T \rightarrow$image of T_2 (with appropriate choice of the isomorphism γ). One sees, using Proposition 9 (i) that δ is an isomorphism. Note that in the context of special dihedral extensions studied in [M] it was also shown that R^0 is isomorphic to a power series ring on one variable over $\boldsymbol{Z}_p$, but its structure as Λ-algebra was not completely determined. In particular, its *rank* over Λ was not known. For representations $\bar{\rho}$ attached to generic admissible S_3-extensions we have just shown this rank to be 1. We also obtain, in our context, as in [M] the result that every ordinary lifting of $\bar{\rho}$ to $\boldsymbol{Z}_p$ is pro-modular (i.e., comes from a p-adic, p-ordinary, cuspidal eigenform).

3.4. The size of the image of Galois for the universal ordinary representation

Let $\rho^0 \colon G \rightarrow GL_2(\boldsymbol{Z}_p[[T]])$ denote the universal ordinary representation for $\bar{\rho}$. In terms of T_1, T_2, T_3, T_2 maps to T while g and T_1 map to 0 in $\boldsymbol{Z}_p[[T]]$. The specialization $T \mapsto 0$ produces the lift of $\bar{\rho}$ with image S_3. Call this lift ρ_0.

Proposition 14. *$\rho^0(G) \cap SL_2(\boldsymbol{Z}_p[[T]])$ is the full inverse image under $T \mapsto 0$ of the subgroup of order 3 of $\rho_0(G)$.*

Proof. The images under ρ^0 of u, $\tau(u)$, $\tau^2(u)$, and v are respectively

$$\begin{pmatrix} 1 & 0 \\ 0 & 1+T \end{pmatrix}, \quad \begin{pmatrix} 1+\frac{3}{4}T & \frac{1}{4}T \\ \frac{3}{4}T & 1+\frac{1}{4}T \end{pmatrix}, \quad \begin{pmatrix} 1+\frac{3}{4}T & -\frac{1}{4}T \\ -\frac{3}{4}T & 1+\frac{1}{4}T \end{pmatrix}, \text{ and} \tag{3.2}$$
$$\begin{pmatrix} (1-3h^2)^{1/2} & h \\ -3h & (1-3h^2)^{1/2} \end{pmatrix}$$

where h is a power series in T such that T_3 maps to $h(T)$. Note that

$h(0)=0$ implies that $h(T)=cT \pmod{T^2}$ ($c \in Z_p$) and by Proposition 10 $c \equiv -1 \bmod p$.

Let the image of $\rho^0(G) \cap SL_2(Z_p[[T]])$ in $SL_2(Z_p[[T]]/(T^n))$ be denoted G_n.

Lemma 10. *The kernel of the mapping*

$$SL_2(Z_p[[T]]/(T^n)) \longrightarrow SL_2(Z_p[[T]]/(T^{n-1}))$$

is contained in G_n $(n \geq 2)$.

Proof. The above-mentioned kernel is generated by the images of the matrices

$$(3.3) \qquad \begin{pmatrix} 1+T^{n-1} & 0 \\ 0 & 1-T^{n-1} \end{pmatrix}, \quad \begin{pmatrix} 1 & T^{n-1} \\ 0 & 1 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ T^{n-1} & 1 \end{pmatrix}.$$

We prove the lemma inductively, as follows. For $n=2$ one notes that the matrices of (3.3) can be obtained as suitable products of matrices in (3.2). For $n \geq 3$, the image of

$$\begin{pmatrix} 1+T^{n-1} & 0 \\ 0 & 1-T^{n-1} \end{pmatrix}$$

in $SL_2(Z_p[[T]]/(T^n))$ may be obtained, for example, as the commutator of matrices

$$\begin{pmatrix} 1 & T \bmod T^2 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ T^{n-2} \bmod T^{n-1} & 1 \end{pmatrix}$$

and the two other matrices in (3.3) may be obtained similarly.

Our proposition then follows.

Remark. This proposition might be contrasted with the results concerning the "fullness of the image of Galois" under ordinary representations whose residual representations contain $SL_2(F_p)$, as proved in [M-W].

References

[B] Boston, N., Deformation theory of Galois representations, Harvard PhD. Thesis, 1987. See also forthcoming publications.

[I] Iwasawa, K., "On Galois groups of local fields." Trans. Amer. Math. Soc., **80** (1955), 448–469.

[K] Koch, H., Galoissche Theorie der p-Erweiterungen. Springer-Verlag, Berlin-Heidelberg-New York, 1970.

[M] Mazur, B., Deforming Galois representations, to appear in the Proceedings of the March 1987 Workshop on "Galois Groups over Q "held at the MSRI, Berkeley, California.

[M-W] Mazur, B. and Wiles, A., On p-adic analytic families of Galois representations, Compositio Math., **59** (1986), 231–264.

[N] Neumann, O., "On p-closed number fields and an analogue of Riemann's existence theorem." In Algebraic Number Fields, Academic Press, London 1977 (Fröhlich, ed.), 625–647.

[P] Pieper, H., "Die Einheitengruppe eines zahm-verzweigten Galoisschen lokalen Körpers als Galois-modul." Math. Nachr., **54** (1972), 173–210.

[T] Tate, J., Les conjectures de Stark sur les fonctions L d'Artin en $s=0$: notes d'un cours à Orsay redigées par Dominique Bernardi et Norbert Schappacher. Birkhäuser, Boston 1984.

Department of Mathematics
Harvard University
Cambridge, MA 02138
U.S.A.