ACTA ARITHMETICA
101.3 (2002)

Deformations of Galois representations arising from degenerate extensions

by

Adam Logan (Berkeley, CA)

1. Introduction. This paper is inspired by that of Boston and Mazur [B-M], and work on this problem was begun when the author was a graduate student of Barry Mazur (supported by an NSF Graduate Fellowship). In [B-M], the authors study the deformation theory of a certain type of S_3-extensions of $\mathbb{Q}$, which they term *neat*, and more specifically that of *generic* S_3-extensions, which satisfy an additional condition. Restricting their numerical study to one particular family of neat extensions, they note that all such extensions seem to satisfy their genericity condition.

Their main result on generic S_3-extensions can be summarized as follows:

Theorem 1.1 [B-M, Prop. 13]. *Let $L/\mathbb{Q}$ be a neat S_3-extension for the prime p* (we will define this in Section 2, below; it has to do with the class number and units of the field L)*. The universal deformation ring of the natural representation of its Galois group into* $\mathrm{GL}_2(\mathbb{F}_p)$ *is isomorphic to* $\mathbb{Z}_p[[T_1, T_2, T_3]]$*. If $L/\mathbb{Q}$ is generic, then*:

(1) *The inertially reducible locus is composed of the union of two smooth hypersurfaces in the universal deformation space.*

(2) *The globally dihedral locus is equal to the inertially dihedral locus and is a smooth hypersurface.*

(3) *The ordinary locus consists of a smooth analytic curve in the deformation space.*

(4) *The inertially ample locus is equal to the complement of the union of three hypersurfaces*, *any two of which meet transversely.*

They also show that generic S_3-extensions actually exist:

Proposition 1.2 [B-M, Prop. 9]. *Let $a \in \mathbb{Z}$ be such that $27 + 4a^3$ is positive*, *prime*, *and less than 10^4. Then the splitting field of the polynomial*

2000 *Mathematics Subject Classification*: Primary 11F80; Secondary 11R32.

x^3+ax+1 *is a generic* S_3*-extension for the prime* $27+4a^3$. (I have verified this for $27+4a^3 < 10^{15}/2$.)

The purpose of this paper is to remove some hypotheses from these statements, at the usual cost of obtaining slightly weaker results. We still let $L/\mathbb{Q}$ be a neat S_3-extension for the prime p and characterize the universal deformation ring of the natural $\mathrm{GL}_2(\mathbb{F}_p)$-representation of its Galois group as isomorphic to $\mathbb{Z}_p[[T_1,T_2,T_3]]$.

THEOREM 1.3. *With hypotheses as above*:

(1) *The inertially reducible and ordinary loci are as in the generic case.*

(2) *The inertially dihedral locus is either a smooth hypersurface or the union of two smooth hypersurfaces.*

(3) *If the inertially dihedral locus is a smooth hypersurface*, *then the inertially ample locus is the complement of the union of the inertially reducible and inertially dihedral loci*, *and is thus the complement of the union of three smooth hypersurfaces.*

In addition, we will give two examples of degenerate S_3-extensions, one of them the splitting field of the polynomial $x^3+7x-12$.

I would like to thank Barry Mazur and Nigel Boston for discussions of this problem, Fernando Gouvêa for encouraging me to pursue it after a long hiatus, and Kenneth Ribet for encouragement and comments on a previous draft of this work. Calculations in this paper were done using gp and the tables of number fields prepared at the Université de Bordeaux. Currently I am supported in part by a VIGRE grant.

2. Basics. We start with some fundamental definitions borrowed from [B-M], with very slight modifications.

DEFINITION (cf. [B-M, Definition 2]). Let $L/\mathbb{Q}$ be a totally complex S_3-extension in which p splits as $(\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^2$, and let S be the set of finite ramified primes of L. We say that L is *admissible* for p, or that L is *neat*, if:

1. Any global unit of L which is locally a pth power at all elements of S is globally a pth power.

2. The class number of L is prime to p.

3. The completion of L at any element of S does not contain pth roots of 1. (In particular, it follows that the cardinality of the residue field is not congruent to 1 mod p.) Let L be a neat S_3-extension of $\mathbb{Q}$, and let $\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3$ be the primes of L lying above p. Let e_1,e_2 be a basis for global units mod pth powers. Since we are assuming that L is neat, we may suppose that e_1 is not a pth power in $L_{\mathfrak{p}_1}$, and we may also arrange things so that e_2 is not a pth power in $L_{\mathfrak{p}_2}$ or $L_{\mathfrak{p}_3}$. If e_2 is not a pth power in $L_{\mathfrak{p}_1}$ either, then L is called *generic*; if it is, L is *degenerate*.

DEFINITION. The *degeneracy index* of L at p is the largest integer i such that e_2 is a p^ith power in $L_{\mathfrak{p}_1}$. Of course this is a finite number, for the only nonzero elements of $L_{\mathfrak{p}_1}$ which are p^ith powers for all i are $(p-1)$st roots of 1.

The authors of [B-M] pay particular attention to the Galois closures of cubic fields of the form $\mathbb{Q}(x)$, where $x^3 + ax + 1 = 0$, for a an integer such that $27 + 4a^3$ is positive and prime. They show that the first seven such fields are generic S_3-extensions of $\mathbb{Q}$, using a simple numerical criterion. As noted above, I have extended this verification to all $a < 500000$, and I do not believe that there are any counterexamples. However, if one does not restrict to these particular cubic fields, it becomes easy to find degenerate S_3-extensions. The tables of number fields available by anonymous FTP from `megrez.math.u-bordeaux.fr` greatly facilitate such a search.

The rest of the paper will be devoted to modifying the proofs and results of Boston and Mazur so that they apply in the degenerate case. That is, we will determine the natural subspaces of the universal deformation space, just as they do in their generic situation.

3. Definitions and notations. We now recall some more definitions from [B-M].

DEFINITION. Let L be an S_3-extension of $\mathbb{Q}$, and let p be a rational prime greater than 3 which decomposes in L as $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$. (We assume that such a prime exists.) Let S be the set of ramified primes of L. Let P be the Galois group over L of the maximal pro-p extension of L unramified away from p, or outside S (in the situations we will be considering, these are the same), G its Galois group over $\mathbb{Q}$, L_p the completion of L at $\mathfrak{p}_1$, P_p the Galois group over L_p of its maximal pro-p extension, and G_p the Galois group of the maximal pro-p extension of L_p over $\mathbb{Q}_p$. We also fix an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_p$, and thus of $\mathrm{Gal}(\bar{L}_p/L_p)$ into $\mathrm{Gal}(\bar{L}/L)$, such that the inertia subgroup P_p^0 maps to the inertia subgroup for $\mathfrak{p}_1$.

PROPOSITION 3.1. *P is a free pro-p group on 4 generators, and P_p is a free pro-p group on 3 generators.*

Proof. [B-M, Props. 3, 4]. ■

We take σ (resp. τ) to be an element of order 2 (resp. 3) in S_3. Following one of the notations in [B-M], we will let P be generated by $u, \tau(u), \tau^2(u), v$, where u conjugated by τ is, obviously, $\tau(u)$, $\tau(v) = v$, $\sigma(u) = u$, and $\sigma(v) = v^{-1}$. On the other hand, P_p will be generated by ξ, η, ϕ, with ξ and η generating the inertia and the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ acting as $+1$ on ξ, ϕ and -1 on η.

Definition. Let E be the group of global units of L. It is the direct product of a free abelian group of rank 2 with a cyclic group of order 2. For any place v of L, let E_v be the group of units in the ring of integers of L_v.

Definition. For any topological group T, let $\overline{T}$ be its p-Frattini quotient. More generally, let ${}_i\overline{T}$ be the maximal quotient of T which is an abelian pro-p group with exponent dividing p^i (that is, ${}_i\overline{T} = T/(T,T)T^{p^i}$).

Definition. Let K be a cubic extension of $\mathbb{Q}$. Let L be its Galois closure, and let S be the set of finite ramified primes of L. Global class field theory gives us a map from the idèle class group of L to the abelianization of its absolute Galois group. This induces a map $\bigoplus_{v\in S}\overline{E}_v \to \overline{P}$ which is trivial on the image in $\bigoplus_{v\in S}\overline{E}_v$ of the global units. Under the conditions that the class number of L be prime to p and that no completion of L at a prime in S contain the pth roots of 1, this map is surjective.

In this situation we say, as above, that L is *neat* for p, or for S, if the map $\overline{E} \to \bigoplus_{v\in S}\overline{E}_v$ is injective. In this case, we consider a map $\overline{E} \to \overline{E}_1$. If it too is injective, we are in the *generic* situation treated by Boston and Mazur. Otherwise, the extension is termed *degenerate*, as remarked above, and the degeneracy index is the largest i for which the map ${}_i\overline{E} \to {}_i\overline{E}_1$ has cyclic image.

The following proposition allows us to check whether the hypotheses on the unit group of L are satisfied by studying the field K. This has obvious advantages when using a computer to determine whether a S_3-extension is generic.

Proposition 3.2. *Let K be a nonreal cubic field as above with fundamental unit ε. If ε is not a pth power in the completion of K at the ramified place above p, then neither is it a pth power in the completion of L at some place above p. Moreover, in this situation ε and its conjugates generate a subgroup of the unit group of L of index prime to p.* (*We are still assuming* $p > 3$.)

Proof. The first statement is obvious, because a place of L above p can be found in which ε is the same as it was in the completion of K. To prove the second, suppose to the contrary that η is a unit of K with $\eta^p = \pm\varepsilon_1^{a_1}\varepsilon_2^{a_2}$. In one place above p, the unit ε_1 is a pth power and ε_2 is not; thus $p \mid a_2$. Similarly, $p \mid a_1$. Therefore $\eta^p = \pm 1$. Since $\eta \in L$, a quadratic extension of a nonreal cubic field, this implies that $p \le 4$, contradiction.

At this point we give an example of a degenerate S_3-extension.

Example 3.3. Let K be the field $\mathbb{Q}(x)$, where $x^3 + 7x - 12 = 0$, and L its Galois closure. We claim that L is a degenerate S_3-extension of $\mathbb{Q}$, of degeneracy index 1, with $p = 5$. Here the set of ramified primes is $\{5, 263\}$, both of which split as $(\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^2$, so it is easy to check that the completions there do not contain fifth roots of 1. The class number of L is 2.

Using gp, it is not hard to check that the units of the cubic subfields of L generate the full unit group of K. A fundamental unit of K is $14x-19$. K has a unique embedding into $\mathbb{Q}_5$, in which the image of x is congruent to 62 mod 125, so that the image of the fundamental unit is congruent to -1 mod 25, but not mod 125, so is a fifth power but not a 25th power. I assert that the image of x under the embedding of K into $\mathbb{Q}_5(\sqrt{10})$ is not a fifth power. This will essentially complete the verification of neatness.

In fact, it is easy to show that a unit of $\mathbb{Q}_5(\sqrt{10})$ which is congruent to 1 modulo $\mathfrak{m}$, the maximal ideal, is a fifth power if and only if it is congruent to 1 modulo $\mathfrak{m}^3$. However, a root of $x^3+7x-12$ which does not belong to $\mathbb{Q}_5$ is congruent modulo $\mathfrak{m}^2$ to $4\pm\sqrt{10}$, and thus the unit is congruent modulo $\mathfrak{m}^2$ to $2\mp\sqrt{10}$ and cannot be a fifth power (multiply by 3^5).

So, if we take a unit $u=\pm u_1^a u_2^b$ of L, where u_1, u_2 are fundamental units in different cubic subfields of L, then in one completion u is a fifth power if and only if $5\,|\,a$, and in another if and only if $5\,|\,b$. Thus u is a fifth power locally if and only if it is a fifth power globally, which finishes the proof that L is neat.

Example 3.4. We attempt to find polynomials giving degenerate extensions of any index. Let p be a prime and n a positive integer; we consider polynomials of the form $f(x)=x^3-rx^2+sx-1$, where r and s are integers congruent mod p^{n+1} to $-(p-1), (p-1)$ respectively. If $r\neq s$, this polynomial is irreducible. Its discriminant is congruent mod p^{n+1} to the discriminant of $x^3-(p-1)x^2+(p-1)x-1$, which is congruent mod p^2 to $-64p$. Let K be the root field of this polynomial; from this, $p\,\|\,D_{K/\mathbb{Q}}$ and so p decomposes in K as $\mathfrak{p}_1^2\mathfrak{p}_2$.

Clearly K has a unit ε congruent to 1 modulo p^{n+1} in the embedding of K into $\mathbb{Q}_p$. This must be the p^nth power of a local unit. On the other hand, if we embed K into $\mathbb{Q}_p(\sqrt{-p})$, the image of ε will never be a pth power. To see this, observe that the root of $f(x)$ is congruent mod p^{n+1} to $1-(r+s)/(3+2r+s)$. Removing this linear factor from $f(x)$ over $\mathbb{Q}_p$, we obtain a polynomial congruent mod p^{n+1} to

$$x^2+\left(r+1-\frac{r+s}{3+2r+s}\right)x+\frac{3+2r+s}{3+r}.$$

But p divides the discriminant of this polynomial exactly, and so the root is of the form $t+u\sqrt{-p}$, with $p\nmid u$. Such a quantity is never a pth power.

Experiments in producing degenerate extensions for various primes p and indices n have been successful; we mention only the case $p=5$, $n=2$, for which the choice $r=-4$, $s=129$ works, the class number of L in this case being $3048192=2^8 3^5 7^2$. However, if we took $s=254$ instead, the field obtained would have class number a multiple of 5 (to be precise, $73170700 = 2^2 5^2 67^2 163$).

4. Representation theory. Let G be a finite group and F a field of characteristic prime to $\operatorname{card} G$. Then, of course, the group algebra $F[G]$ is semisimple. It is isomorphic to a direct sum of matrix algebras over F if and only if all irreducible representations of G (say there are c of them) can be defined over F.

Suppose we are in this case, and let R be a local Artinian ring with residue field F. Since $R[G] \cong F[G] \otimes_F R$, it is clear that $R[G]$ is likewise a direct sum of c matrix algebras. Now, representations of G with coefficients in R correspond naturally to $R[G]$-modules free over R. These, then, correspond to R^c-modules free over R, that is, to c-tuples of free R-modules. In turn, these correspond canonically to c-tuples of F-modules, whence to $F[G]$-modules or to representations. In summary, a representation of G in $M_n(R)$ is uniquely determined up to conjugacy by its reduction to $M_n(F)$. The usual theorems on reducibility of representations then follow for representations to R. For example, if we have a representation ϱ to R which is an extension of representations, it must in fact be their sum, for ϱ and the sum have the same reduction to $M_n(F)$.

We will apply these ideas with $F = \mathbb{F}_p$ and $G = S_3$. In essence, they allow us to immediately take over all results about module decompositions given in [B-M] without change here. Since P, the Galois group of the maximal pro-p extension of L unramified away from p over L, is a free pro-p group, the groups ${}_i\overline{P}$ are all free modules over $\mathbb{Z}/p^i\mathbb{Z}$ of the same rank.

Proposition 4.1. *A is a semidirect product of P by S_3 such that for any j, A acts on ${}_j\overline{P}$ by $V+\chi$, where χ is the nontrivial 1-dimensional representation of S_3 with coefficients in $\mathbb{F}_p$ and V is the natural 3-dimensional representation of S_3. For any j, A_p is a semidirect product of P_p by $\mathbb{Z}/2\mathbb{Z}$, with $\mathbb{Z}/2\mathbb{Z}$ acting on ${}_j\overline{P}_p$ by $1+1+\chi$. In the global case, the inertia subgroup maps to the space spanned by a basis vector of V and χ (not a submodule, since different choices of prime above p give different inertia subgroups); in the local case, to $1+\chi$.*

Proof. [B-M, Props. 7 and 8], together with the above to remove the restriction $j = 1$ made there. ■

Boston and Mazur study the exact sequence of p-Frattini quotients

$$0 \to \overline{E} \to \overline{E}_1 \oplus \overline{E}_2 \oplus \overline{E}_3 \to \overline{P} \to 0.$$

Likewise we will study the exact sequence of p^i-quotients. That is, we define a map Π^i_j to be that given by class field theory from ${}_j\overline{E}_k$ to ${}_j\overline{P}$. Its image will be denoted ${}_j\overline{P}_k$, and by class field theory ${}_j\overline{P}_1$ is the image of the inertia subgroup ${}_j\overline{P}{}_p^0$ in ${}_j\overline{P}$.

PROPOSITION 4.2. *Let L be an S_3-extension of $\mathbb{Q}$, degenerate for p with degeneracy index i. Then the intersection of any two, or all three, of the ${}_j\overline{P}_k$ is isomorphic to $\mathbb{Z}/p^l\mathbb{Z}$, where $l = \min(i,j)$.* (In the case $j = 1$, this reduces to the results in the first part of [B-M, Section 2.3].)

Proof. We consider the cases $i < j$, $j \le i$ separately. In the case $j \le i$, the image of P_1 is isomorphic to $\mathbb{Z}/p^j\mathbb{Z}$, and it is stable under the action of the involution of the Galois group which fixes $\mathfrak{p}_1$. The rest of the proof in [B-M, Section 2.3] can now be taken over word for word.

We now consider the case $i < j$. Everything is compatible with the inclusion maps ${}_j\overline{E}_k \to {}_{j+1}\overline{E}_k$ and ${}_j\overline{P} \to {}_{j+1}\overline{P}$, so the image must contain a $\mathbb{Z}/p^i\mathbb{Z}$-subgroup, and no more elements of order dividing p^i. If there is an element of higher order in the intersection ${}_j\overline{P}_k \cap {}_j\overline{P}_{k'}$, say y, coming from y_k and $y_{k'}$, then the element $y_k \oplus y_{k'} \oplus 0$ would be in the image of ${}_j\overline{E}$, by exactness. This would immediately imply that the degeneracy index of L is greater than i. ∎

5. Linking local and global presentations. We have already described (in Propsition 4.1) the presentations of the local and global Galois groups G_p, G. Now we must show how they behave under the map $G_p \to G$ (in particular, what happens when we restrict this to a map $\Pi_p \to \Pi$). Here the difference between the generic and degenerate situations becomes important.

PROPOSITION 5.1 (cf. [B-M, Lemma 2.4.4]). *Suppose that i, the degeneracy index of L, is at least j, and let ξ, η be generators of the inertia subgroup of ${}_j\overline{P}_p$ such that the nontrivial element of* $\mathrm{Gal}(L_p/\mathbb{Q})$ *acts as $+1$ on ξ and -1 on η. Let r, s be the images of ξ, η in ${}_j\overline{\Pi}$, and let R, S be the S_3-stable subspaces that they generate. Then $R \cong 1 + \varepsilon$ and $S \cong \chi$.*

Proof. Recall that ${}_j\overline{\Pi} \cong 1 + \chi + \varepsilon$. Because L has no unramified extensions of degree p, the S_3-stable subspace of ${}_j\overline{\Pi}$ generated by the image of a local inertia group—that is, $R + S$—must be the whole thing. Also, R, S must be quotients of the inductions of 1 and χ from $A_p = \mathbb{Z}/2\mathbb{Z}$ to $A = S_3$, respectively. On the other hand, if $i < j$, neither R nor S can be one-dimensional over $\mathbb{Z}/p^j\mathbb{Z}$, by Proposition 4.2. Thus, the statement on R follows if we prove the statement about S.

We let a and b be generators of ${}_j\overline{E}_1$ corresponding to ξ and η such that $a^\sigma = a, b^\sigma = 1/b$. Let v be the global unit of L which is a p^jth power in $L_{\mathfrak{p}_1}$. Then the image of v in ${}_j\overline{E}_{\mathfrak{p}_2}$ must be a multiple of b. Indeed, on the one hand, the product of the three global conjugates of v can be taken to be 1, and on the other hand, the two conjugates that are not in $\mathbb{Q}_p$ are local conjugates in L_p, so when reduced to ${}_j\overline{E}_{L_p}$ they have the same coefficient of a, which must therefore be 0. On the other hand, the coefficient of b must be a unit, for otherwise v would be a pth power everywhere locally, a possibility excluded by our hypotheses.

In particular, the image of ${}_j\overline{E}_L$ in $\bigoplus_k {}_j\overline{E}_k$ is spanned by $(b,-b,0)$ and $(0,b,-b)$. It follows that the intersection of the images of the ${}_j\overline{E}_k$ in ${}_j\overline{P}$ is the image of $(b,0,0)$, which is obviously the χ subspace as claimed. ∎

A curious consequence of this proposition is as follows:

COROLLARY 5.2. *Let $L/\mathbb{Q}$ be an S_3-extension of degeneracy index at least j for p, and let F be the subextension of $\mathbb{Q}(\zeta_{p^{j+1}})$ which is of degree p^j over $\mathbb{Q}$. Then the class group of the compositum FL contains a subgroup isomorphic to $(\mathbb{Z}/p^j\mathbb{Z})^2$.*

Proof. It is sufficient, of course, to construct an unramified extension with this Galois group. The point is simply that the inertia groups for $\mathfrak{p}_i$ in the extension cut out by ${}_j\overline{P}$ are isomorphic to $(\mathbb{Z}/p^j\mathbb{Z})^2$ and have an intersection isomorphic to $(\mathbb{Z}/p^j\mathbb{Z})$, which cuts out the extension M, say. On the other hand, $FL \subset M$ and is totally ramified over L at each $\mathfrak{p}_i$. Thus, M/FL is unramified at these primes, and (by definition of P) at all others as well. ∎

We must now specify the relation between local and global presentations more precisely.

PROPOSITION 5.3 (cf. [B-M, Prop. 10]). *Assume that $L/\mathbb{Q}$ is an admissible S_3-extension of degeneracy index i for the prime p. Then we may take the local and global systems of generators such that the image of ξ is u and, in the induced map on quotients ${}_j\overline{\Pi}_p \to {}_j\overline{\Pi}$, the image of η is v, if $i \geq j$.*

Proof. By [B-M, Prop. 7 and addendum] we may take the image of ξ to be u. The statement about η follows from the last lemma, similarly to the proof of [B-M, Prop. 10]. ∎

We have now accumulated all necessary information about the Galois groups and can proceed to studying the universal deformation.

6. The universal deformation. As before, let $L/\mathbb{Q}$ be an admissible S_3-extension; for the moment, the index of degeneracy does not matter. There is a Galois representation $\overline{\varrho} : G \to \mathrm{GL}_2(\mathbb{F}_p)$, unique up to conjugacy, which factors through $\mathrm{Gal}\, L/\mathbb{Q}$ and maps it injectively into $\mathrm{GL}_2(\mathbb{F}_p)$. For concreteness, we fix elements σ, τ in S_3 of order 2 and 3 respectively and map them to

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1/2 & 1/2 \\ -3/2 & -1/2 \end{pmatrix}.$$

We will be studying deformations of $\overline{\varrho}$ to complete local noetherian rings with residue field $\mathbb{F}_p$. The universal deformation has been completely described.

PROPOSITION 6.1. *The universal deformation ring is the power series ring $\mathbb{Z}_p[[T_1, T_2, T_3]]$, and the universal deformation may be given as follows*:

$$\sigma \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \tau \mapsto \begin{pmatrix} -1/2 & 1/2 \\ -3/2 & -1/2 \end{pmatrix},$$

$$u \mapsto \begin{pmatrix} 1+T_1 & 0 \\ 0 & 1+T_1 \end{pmatrix}, \quad v \mapsto \begin{pmatrix} (1-3T_3^2)^{1/2} & T_3 \\ -3T_3 & (1-3T_3^2)^{1/2} \end{pmatrix}.$$

Proof. This is [B-M, Prop. 11], and a detailed proof is given there. ∎

To understand the universal deformation more fully, we must understand the image of η. Since η conjugated by σ is η^{-1}, the image of η must have determinant 1 and equal diagonal entries, so it is, say,

$$\begin{pmatrix} (1+fg)^{1/2} & f \\ g & (1+fg)^{1/2} \end{pmatrix}.$$

PROPOSITION 6.2. *Modulo $\mathfrak{m}$, the power series f is congruent to T_3, and g to $-3T_3$.*

Proof. As [B-M, Prop. 12], except that here the image of ${}_1\overline{\eta}$ under the natural map $\overline{\Pi}_p \to \overline{\Pi}$ is $\overline{v}$. ∎

We can now determine some of the natural subspaces. We will be considering representations of the Galois group into $\mathrm{GL}_2(\mathbb{Z}_p)$ which are deformations of the representation into $\mathrm{GL}_2(\mathbb{F}_p)$. Thus they come from the universal deformation, and are described by a continuous homomorphism $\mathbb{Z}_p[[T_1, T_2, T_3]] \to \mathbb{Z}_p$. Such a homomorphism α is described by giving $\alpha(T_1), \alpha(T_2), \alpha(T_3)$; the space of such is therefore naturally identified with $p\mathbb{Z}_p \times p\mathbb{Z}_p \times p\mathbb{Z}_p$, which is a 3-dimensional p-adic manifold. The only visible difference between our situation and the generic one is that here f and g are not transversal.

PROPOSITION 6.3 (cf. [B-M, Prop. 13]). *The inertially reducible locus is the union of the hypersurfaces $f = 0$ and $g = 0$. The ordinary locus is the smooth curve defined by $T_1 = g = 0$.*

Proof. Identical to the proofs given in [B-M]. ∎

It is still true that a representation is inertially dihedral if and only if $T_1 = T_2$ or $f = g = 0$.

7. Problems. This work leaves several questions unanswered, such as the following:

(1) It would be of interest to have such concrete descriptions of deformation loci under weaker hypotheses. Thus, what happens when the class number is a multiple of p or if there are units that are pth powers everywhere locally but not globally?

(2) For each prime p and positive integer n, construct an S_3-extension of $\mathbb{Q}$ with degeneracy index n at p. The construction of Example 3.4 works well in practice. It is unclear, though, how to make sure that an extension of class number prime to p can always be found; and it seems more difficult still to prevent primes congruent to 1 mod p from being ramified.

(3) Prove that the order of contact of the loci defined by $f = 0$ and $g = 0$ is equal to the degeneracy index of the extension. From this it would follow that the inertially ample locus is the complement of the union of inertially reducible and inertially dihedral loci, by the same argument as in [B-M].

Reference

[B-M] N. Boston and B. Mazur, *Explicit universal deformations of Galois representations*, in: Algebraic Number Theory, J. Coates *et al.* (eds.), Adv. Stud. Pure Math. 17, Academic Press and Kinokuniya, 1989, 1–21.

Department of Mathematics
University of California
970 Evans Hall
Berkeley, CA 94720-3840, U.S.A.
E-mail: adam@math.berkeley.edu

Received on 23.3.2001 (4005)