PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 5, May 2009, Pages 1551–1560
S 0002-9939(08)09677-9
Article electronically published on November 14, 2008

CAPPING GROUPS AND SOME CASES OF THE FONTAINE-MAZUR CONJECTURE

FRAUKE M. BLEHER, TED CHINBURG, AND JENNIFER FROELICH

(Communicated by Ken Ono)

ABSTRACT. In this paper we will prove some cases of the Fontaine-Mazur conjecture. Let p be an odd prime and let $G_{\mathbb{Q},\{p\}}$ be the Galois group over $\mathbb{Q}$ of the maximal unramified-outside-p extension of $\mathbb{Q}$. We show that under certain hypotheses, the universal deformation of the action of $G_{\mathbb{Q},\{p\}}$ on the 2-torsion of an elliptic curve defined over $\mathbb{Q}$ has finite image. We compute the associated universal deformation ring, and we show in the process that $\hat{S}_4$ caps $\mathbb{Q}$ for the prime 2, where $\hat{S}_4$ is the double cover of S_4 whose Sylow 2-subgroups are generalized quaternion groups.

1. INTRODUCTION

This article concerns some cases of the Fontaine-Mazur conjecture. Let L be a number field and suppose that S is a finite set of places of L. Let $G_{L,S}$ be the Galois group of the maximal algebraic extension L_S of L which is unramified outside S. Suppose that k is a perfect field of positive characteristic ℓ. Let $\overline{\rho} : G_{L,S} \to \mathrm{GL}_n(k)$ be a continuous representation of $G_{L,S}$ associated to a continuous $kG_{L,S}$-module V and a choice of basis for V over k, where $n = \dim_k(V) < \infty$. If S contains no places over ℓ, the Fontaine-Mazur conjecture predicts that the image of the versal deformation

$$\rho : G_{L,S} \to \mathrm{GL}_n(R(G_{L,S}, V))$$

of V should be finite, where $R(G_{L,S}, V)$ is the versal deformation ring of V. We will prove that this is the case when $L = \mathbb{Q}$, $S = \{p\}$ consists of a single odd prime, $k = \mathbb{Z}/2$, and $V = E[2]$ is the representation of $G_{\mathbb{Q},S}$ resulting from the Galois action on the 2-torsion of an elliptic curve E defined over $\mathbb{Q}$, provided that certain additional hypotheses are met.

Under these hypotheses, we determine $R(G_{\mathbb{Q},S}, V)$, and we show that the image of ρ is the double cover $\hat{S}_4$ of S_4 whose Sylow 2-subgroups are generalized quaternion groups. We show that, in fact, $\hat{S}_4$ caps $G_{\mathbb{Q},S}$ for $\ell = 2$, in the sense that there are no non-trivial pro-2 quotients of $\mathrm{Ker}(\rho)$. By [1, Lemma 3.3], this is equivalent to the statement that the versal deformation of an arbitrary mod 2 representation of $G_{\mathbb{Q},S}$ which factors through $\hat{S}_4$ is trivial on $\mathrm{Ker}(\rho)$.

Received by the editors April 14, 2008, and, in revised form, June 21, 2008.
2000 *Mathematics Subject Classification.* Primary 11R32; Secondary 20C05, 11G05.
The first author was supported in part by NSA Grant H98230-06-1-0021 and NSF Grant DMS06-51332.
The second author was supported in part by NSF Grant DMS05-00106.

In [1] we showed that S_4 never caps $G_{\mathbb{Q},S}$ for the prime 2 at any set of places S. We were able to show that S_4 does cap $G_{\mathbb{Q}(\sqrt{d}),\emptyset}$ for the prime 2 for infinitely many real quadratic fields $\mathbb{Q}(\sqrt{d})$. The double covers of S_4 are the smallest extensions of S_4 by a two-group which are candidates for capping $G_{\mathbb{Q},S}$ for the prime 2.

The fact that the image of ρ is finite shows that the deformation theory of linear representations of $G_{\mathbb{Q},S}$ does not provide a great deal of information about $G_{\mathbb{Q},S}$. Boston has formulated a generalization of the Fontaine-Mazur conjecture (see [2, 3]) which for all number fields L and prime numbers ℓ for which S contains no place over ℓ would provide more information about pro-ℓ quotients of $G_{L,S}$ via actions of this group on rooted trees.

The S we consider in connection with $V = E[2]$ does not contain either $\ell = 2$ or the infinite place ∞ of $\mathbb{Q}$. This differs from the sets S which arise in the theory of holomorphic modular forms, where the natural deformation conditions require one to include both $\ell = 2$ and ∞ (see [4]). This highlights the following issue concerning Boston's theory of Galois group actions on rooted trees. One would like to know what objects in this theory would play a role analogous to that of modular forms. Such objects would provide numerical invariants, similar to the Fourier coefficients of modular forms, which would describe Galois actions on such trees.

This paper is organized in the following way. In §2 we recall the basic definitions we need concerning deformations, as well as the concept of capping groups from [1]. In §3 we recall some constructions from [1] concerning certain S_4-extensions N of $\mathbb{Q}$ which are unramified outside a single prime p (and unramified at infinity). In §4, we apply results from [1] to show that the above S_4-extensions are contained in $\hat{S}_4$-extensions which are also unramified outside p. We then prove that these $\hat{S}_4$-extensions cap $\mathbb{Q}$ at $S = \{p\}$ for the prime $\ell = 2$, which is our first main result (Theorem 4.2). In §5, we show that for each S_4-extension N as above, there is an elliptic curve E over $\mathbb{Q}$ with the property that when V is the Galois module $E[2]$ of 2-torsion on E, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on V factors through the unique S_3-quotient of $\mathrm{Gal}(N/\mathbb{Q}) = S_4$. As our second main result we determine in Theorem 5.1 the universal deformation ring $R(G_{\mathbb{Q},S}, V)$ for $V = E[2]$ and show that the image of the universal deformation $\rho : G_{\mathbb{Q},S} \to \mathrm{GL}_n(R(G_{\mathbb{Q},S}, V))$ is isomorphic to $\hat{S}_4$. In particular, we show that $R(G_{\mathbb{Q},S}, V)$ is a complete intersection ring.

2. Background and definitions

Suppose k is a field of characteristic $\ell > 0$, W is a complete local commutative Noetherian ring with residue field k, and Γ is a profinite group. Let V be a finite-dimensional $k\Gamma$-module (having the discrete topology and a continuous Γ-action). In [7] Mazur supposed V is absolutely irreducible, while in [5], de Smit and Lenstra made the weaker hypothesis that $\mathrm{End}_{k\Gamma}(V) = k$. Under these respective hypotheses, these authors proved that there is a universal deformation ring $R(\Gamma, V)$ characterized by the following property. Let $\mathcal{C}$ be the category of all topological local commutative W-algebras R with residue field k which are the projective limits of their discrete Artinian quotients. A lift of V over an object R in $\mathcal{C}$ is a pair (M, ϕ) consisting of an $R\Gamma$-module M which is free over R together with a $k\Gamma$-module isomorphism $\phi : k \otimes_R M \cong V$. Isomorphisms between lifts are defined in the natural way, and an isomorphism class of lifts over R is called a deformation of V over R. The deformation functor $\mathcal{F}_V : \mathcal{C} \to \mathrm{Sets}$ sends an object R in $\mathcal{C}$ to the set of all deformations of V over R. Then V has a universal deformation ring $R(\Gamma, V)$ in

$\mathcal{C}$ if the functor $\mathcal{F}_V$ is naturally isomorphic to $\mathrm{Hom}_{\mathcal{C}}(R(\Gamma,V),-)$, i.e. if $R(\Gamma,V)$ represents the functor $\mathcal{F}_V$. (Note that since we have assumed $\mathrm{End}_{k\Gamma}(V)=k$, and the map $R^*\to k^*$ is surjective, the isomorphism class of a lift (M,ϕ) is determined by the isomorphism class of M as an $R\Gamma$-module.)

Suppose now that k is a discrete perfect field of characteristic $\ell>0$ and that Γ satisfies the following ℓ-finiteness condition of Mazur [7]: For every continuous finite-dimensional $k\Gamma$-module X, the k-dimension of $\mathrm{H}^1(\Gamma,X)$ is finite. By [7], this implies that if V is an arbitrary continuous finite-dimensional representation of Γ over k, then the versal deformation ring $R(\Gamma,V)$ is well-defined and Noetherian. In particular, we can take W to be the ring of infinite Witt vectors over k. The versal deformation ring $R(\Gamma,V)$ may not represent the deformation functor $\mathcal{F}_V$, but there exists a lift $(U(\Gamma,V),\phi_U)$ of V over $R(\Gamma,V)$ such that for each complete local commutative Noetherian ring R with residue field k and each lift (M,ϕ) of V over R, there exists a (not necessarily unique) continuous W-algebra homomorphism $\alpha: R(\Gamma,V)\to R$ such that $M\cong R\otimes_{R(\Gamma,V),\alpha}U(\Gamma,V)$.

We now recall the concept of capping groups introduced in [1].

Definition 2.1. Let ℓ be a prime number, and suppose there is a short exact sequence

$$1\to K\to\Gamma\xrightarrow{\pi}G\to 1 \tag{2.1}$$

where Γ and G are profinite groups, π is a continuous group homomorphism and K is a closed normal subgroup of Γ. We say *G caps Γ (via π) for ℓ* if there is no closed normal subgroup K_0 of Γ satisfying $K_0<K$ and for which K/K_0 is a non-trivial pro-ℓ group.

The relationship between capping groups and deformation theory is as follows.

Proposition 2.2 ([1, Lemma 3.3])**.** *Fix a perfect field k of characteristic ℓ. Let $M(\Gamma,G,k)$ be the set of continuous finite-dimensional representations V of Γ over k which are inflated from representations of G. If Γ satisfies Mazur's ℓ-finiteness condition, then the following are equivalent:*

i. *The group G caps Γ via π for ℓ.*
ii. *The group $K=\mathrm{Ker}(\pi:\Gamma\to G)$ acts trivially on $U(\Gamma,V)$ for all $V\in M(\Gamma,G,k)$.*

In particular, if G caps Γ via π for ℓ and $V\in M(\Gamma,G,k)$, then $R(\Gamma,V)$ is isomorphic to the versal deformation ring $R(G,V)$ of V as a representation of G.

Definition 2.3. Let ℓ be a prime, let G be a profinite group, and let L be a number field.

i. We say *G caps L for ℓ at a set of places S* if there exists some π as in (2.1) such that G caps $G_{L,S}$ via π for ℓ, where $G_{L,S}$ denotes the Galois group of the maximal unramified-outside-S extension of L.
ii. We say *G caps L for ℓ* if there is a set of places S such that G caps L for ℓ at S.

The natural question in this context is:

Question 2.4. Given a prime ℓ and a number field L, which profinite groups G cap L for ℓ?

We proved in [1, Theorem 3.7] that the symmetric group S_n caps $\mathbb{Q}$ for $\ell = 2$ if $n = 2, 3$ but does not cap $\mathbb{Q}$ for $\ell = 2$ if $n \geq 4$. We also showed that there are infinitely many real quadratic fields L such that S_4 caps L for $\ell = 2$ at the empty set S of places of L.

3. Certain S_4-extensions of $\mathbb{Q}$

We now recall from [1] the construction of certain S_4-extensions of $\mathbb{Q}$.

Proposition 3.1 ([1, Proposition 6.2])**.** *Let F_4 be a totally real quartic field of odd prime discriminant p. Let N be the Galois closure of F_4 over $\mathbb{Q}$. Then N is an S_4-extension of $\mathbb{Q}$. The quadratic subfield F_2 of N is $\mathbb{Q}(\sqrt{p})$, and $p \equiv 1 \mod 4$. In F_4, p splits as a product $\mathcal{P}_1^2\mathcal{P}_2\mathcal{P}_3$, where the $\mathcal{P}_i$ are degree one primes. The inertia group of a prime over p in N equals the decomposition group of this prime, and is generated by a transposition. Let F_3 be one of the three cubic subfields of N. Then F_3 has discriminant p, and p splits in F_3 as $\mathcal{Q}_1^2\mathcal{Q}_2$, where $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are degree one primes.*

Remark 3.2. The only place of F_3 which ramifies in N is $\mathcal{Q}_2$. The inertia groups of the primes of N over $\mathcal{Q}_2$ are generated by transpositions in $\mathrm{Gal}(N/F_3)$ lying in one conjugacy class in $\mathrm{Gal}(N/F_3)$. These transpositions generate a group H of order 4. Since N^H is an everywhere unramified quadratic extension of F_3, the class number of F_3 is even.

Lemma 3.3 ([1, Lemma 6.3])**.** *Let N be as in Proposition* 3.1*, and suppose that $p \equiv 5 \mod 8$. There is then a unique quadratic extension N' of N which is Galois over $\mathbb{Q}$ such that $\mathrm{Gal}(N'/\mathbb{Q})$ is a central extension of $\mathrm{Gal}(N/\mathbb{Q}) = S_4$ by a group $T = \mathrm{Gal}(N'/N)$ of order 2 and $N'/\mathbb{Q}$ is unramified outside $\{p\}$. In particular, N' is totally real. The field N' is $\mathbb{Q}_{\{p\}}^{\mathrm{Ker}(\rho)}$ when $\rho : G_{\mathbb{Q},\{p\}} \to \mathrm{GL}_2(\mathbb{C})$ is a lifting of a projective representation $\tilde{\rho} : G_{\mathbb{Q},\{p\}} \to \mathrm{PGL}_2(\mathbb{C})$ having $\mathrm{Ker}(\tilde{\rho}) = \mathrm{Gal}(\mathbb{Q}_{\{p\}}/N)$. There are two mutually exclusive possibilities:*

a. *The determinant $\det(\rho)$ is trivial, which happens if and only if the extension N'/N is quadratically ramified at every prime of N over p.*
b. *The determinant $\det(\rho)$ is non-trivial, which happens if and only if the extension N'/N is everywhere unramified.*

In case (b), either the class number of the quartic subfield F_4 of N is even or every element of the unit group $O_{F_4}^*$ is congruent to a square at each of the residue fields $k(\mathcal{P}_2)$ and $k(\mathcal{P}_3)$.

Remark 3.4. It was shown in [1, Proof of Theorem 6.1] that when $p = 14197$, there is a field N as in Proposition 3.1. In this case one can take F_3 to be $\mathbb{Q}(y_1)$ when y_1 is one of the roots of $y^3 - 16y - 9$. The unit $u = 2 + 4y_1 + y_1^2$ of F_3 is not a square at the unique ramified prime $\mathcal{Q}_1$ over p, where $y_1 \cong -7543 \mod \mathcal{Q}_1$. We see using PARI (see [8]) that the class number of F_3 is 2. The quartic field F_4 is $\mathbb{Q}(x_1)$ when x_1 is a root of $g(x) = x^4 - 6x^2 - 3x + 1$. Via PARI, one checks that the class number of F_4 is one, and the unit $1 + x_1$ is not a square modulo the unramified prime $\mathcal{P}_2$ over p for which $x_1 \equiv -5272 \mod 14197$.

4. $\hat{S}_4$-extensions of $\mathbb{Q}$

In this section we prove the following theorem.

Theorem 4.1. *Let $\hat{S}_4$ be the double cover of S_4 whose Sylow 2-subgroups are generalized quaternion groups. Then $\hat{S}_4$ caps $\mathbb{Q}$ for the prime $\ell = 2$.*

More precisely, we will show:

Theorem 4.2. *Suppose $p \equiv 5 \bmod 8$ is a prime for which there is a field N as in Proposition 3.1. With the notations of that Proposition, suppose that the following are true:*

i. *F_4 has odd class number.*
ii. *There is a unit of F_4 which is not a square at some unramified prime of F_4 over p.*
iii. *The class number of F_3 is exactly divisible by 2.*
iv. *There is a unit u of F_3 which is not a square at some prime of F_3 over p.*

Then N is contained in an $\hat{S}_4$-extension N' of $\mathbb{Q}$. The group $\hat{S}_4$ caps $G_{\mathbb{Q},\{p\}}$ for $\ell = 2$ via the resulting surjection $\pi : G_{\mathbb{Q},\{p\}} \to \mathrm{Gal}(N'/\mathbb{Q})$.

Example 4.3. When $p = 14197$, Remark 3.4 shows that the hypotheses of Theorem 4.2 are satisfied.

Proof. By Lemma 3.3 and hypotheses (i) and (ii) of Theorem 4.2, there is a quadratic extension N' of N with the following properties. The field N' is Galois over $\mathbb{Q}$, unramified outside of p, ramified over N at all the primes of N over p, and such that $\mathrm{Gal}(N'/\mathbb{Q})$ is the (unique) central extension of $\mathrm{Gal}(N/\mathbb{Q}) = S_4$ by $\{\pm 1\}$ for which there is a faithful two-dimensional representation $\rho : \mathrm{Gal}(N'/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ with $\det(\rho)$ trivial. The restriction of this ρ to a Sylow 2-subgroup $\Gamma(2)$ of $\Gamma = \mathrm{Gal}(N'/\mathbb{Q})$ is then a faithful two-dimensional representation with trivial determinant of an extension of a dihedral group of order 8 by $\{\pm 1\}$. This implies that $\Gamma(2)$ is a generalized quaternion group of order 16, which in turn implies that $\mathrm{Gal}(N'/\mathbb{Q})$ is isomorphic to $\hat{S}_4$ by [1, Lemma 4.2].

The fields N and N' are contained in the maximal extension $\mathbb{Q}_{\{p\}}$ of $\mathbb{Q}$ which is unramified outside p. Let $G = \mathrm{Gal}(\mathbb{Q}_{\{p\}}/\mathbb{Q})$, and let $H = \mathrm{Gal}(\mathbb{Q}_{\{p\}}/F_3)$. Then H has index 3 in G. Let $H^{(2)}$ be the maximal pro-2 quotient of H, and let $H_{(2)}$ be the kernel of $H \to H^{(2)}$. Thus $H^{(2)}$ is the Galois group over F_3 of the maximal pro-2 extension L of F_3 in $\mathbb{Q}_{\{p\}}$. Because N is a Galois extension of F_3 contained in L, L can also be described as the maximal pro-2 extension of N contained in $\mathbb{Q}_{\{p\}}$. Since N is normal over $\mathbb{Q}$, this implies L is normal over $\mathbb{Q}$, so $H_{(2)}$ is normal in G. Define $G^{(2)} = G/H_{(2)} = \mathrm{Gal}(L/\mathbb{Q})$. To prove Theorem 4.2, it will suffice to show $L = N'$, since then the kernel of the surjection $\pi : G_{\mathbb{Q},\{p\}} \to \mathrm{Gal}(N'/\mathbb{Q})$ can have no non-trivial pro-2 quotient.

The extension N/F_3 has Galois group isomorphic to a dihedral group of order 8. Therefore there is a unique biquadratic extension N'' of F_3 contained in N, and N''/F_3 is unramified outside the prime $\mathcal{Q}_2$ of F_3 since this is true of N/F_3. Thus N''/F_3 produces a Klein four quotient of the group $Cl_{\mathcal{Q}_2}(F_3)$, which lives in an exact sequence

$$1 \to \frac{k(\mathcal{Q}_2)^*}{\mathrm{Image}(O_{F_3}^*)} \to Cl_{\mathcal{Q}_2}(F_3) \to Cl(F_3) \to 1. \tag{4.1}$$

By hypothesis (iii), 2 exactly divides the order of $Cl(F_3)$. Therefore every unit of $O_{F_3}^*$ must be a square in $k(\mathcal{Q}_2)^*$. In particular, this is true of the unit u in hypothesis (iv).

The Galois group over F_3 of the maximal pro-2 abelian extension of F_3 which is unramified outside the two primes $\mathcal{Q}_1$ and $\mathcal{Q}_2$ of F_3 over p is isomorphic to a Sylow 2-subgroup of the ray class group $Cl_{\mathcal{Q}_1\mathcal{Q}_2}(F_3)$. We claim that this Sylow 2-subgroup is isomorphic to $(\mathbb{Z}/2)^2$. We have an exact sequence

$$1 \to \frac{k(\mathcal{Q}_1)^* \times k(\mathcal{Q}_2)^*}{\text{Image}(O_{F_3}^*)} \to Cl_{\mathcal{Q}_1\mathcal{Q}_2}(F_3) \to Cl(F_3) \to 1 \tag{4.2}$$

where $O_{F_3}^*$ is mapped diagonally into the residue fields of $\mathcal{Q}_1$ and $\mathcal{Q}_2$. The group $O_{F_3}^*$ contains -1 and the unit u in hypothesis (iv). Since $p \equiv 5 \bmod 8$, the Sylow 2-subgroups of each of $k(\mathcal{Q}_1)^*$ and $k(\mathcal{Q}_2)^*$ have order 4, and -1 is a square but not a fourth power in each of these groups. By hypothesis (iv), u is not a square at some prime over p in F_3, but we have shown already that it must be a square at $\mathcal{Q}_2$, so it is not a square at $\mathcal{Q}_1$. Thus the image of u in the maximal two-quotient of $k(\mathcal{Q}_1)^* \times k(\mathcal{Q}_2)^*$ generates a cyclic group of order 4 which does not contain the image of -1 in this quotient, since if -1 were in the image, it would have to be the image of u^2, but u^2 is a fourth power in $k(\mathcal{Q}_2)^*$. Thus $\text{Image}(O_{F_3}^*)$ has order at least 8 in the maximal two-quotient of $k(\mathcal{Q}_1)^* \times k(\mathcal{Q}_2)^*$. We can now conclude that the Sylow 2-subgroups of the group $\dfrac{k(\mathcal{Q}_1)^* \times k(\mathcal{Q}_2)^*}{\text{Image}(O_{F_3}^*)}$ have order at most 2. Thus (4.2), together with our hypothesis that 2 exactly divides the class number of F_3, implies that the Sylow 2-subgroups of $Cl_{\mathcal{Q}_1\mathcal{Q}_2}(F_3)$ have order at most 4. So the existence of the biquadratic extension N'' of F_3 implies that these Sylow 2-subgroups are isomorphic to $(\mathbb{Z}/2)^2$.

We conclude that the maximal abelian quotient of the pro-2 group $H^{(2)}$ is isomorphic to $(\mathbb{Z}/2)^2$. On the other hand the extension N' of F_3 shows that $H^{(2)}$ has a quotient isomorphic to a generalized quaternion group of order 16. Thus if T is any finite quotient group of $H^{(2)}$ which has $\text{Gal}(N'/F_3)$ as a quotient, then $T^{ab} = (\mathbb{Z}/2)^2$ and T has a generalized quaternion quotient. It is shown in [6, Theorem 4.5 of Chapter 5] that $T^{ab} = (\mathbb{Z}/2)^2$ forces T to be a dihedral 2-group, a generalized quaternion 2-group or a semi-dihedral 2-group. However, the only groups of this kind which have a generalized quaternion quotient are generalized quaternion 2-groups, and an elementary argument using generators and relations shows that all proper quotients of a generalized quaternion 2-group are dihedral. So we conclude that $H^{(2)} = \text{Gal}(N'/F_3)$ is a generalized quaternion group of order 16. Thus $G^{(2)} = \text{Gal}(N'/\mathbb{Q})$ and the field L discussed above is the field N', which completes the proof. □

5. Universal deformation rings

Throughout this section we will suppose that p and N satisfy the conditions of Theorem 4.2. There is then, up to isomorphism, a unique two-dimensional irreducible representation V of $\text{Gal}(N/\mathbb{Q}) = S_4$ over $k = \mathbb{Z}/2$. This representation can be described in the following way.

Let x be an element of the cubic subfield F_3 of N which generates F_3 over $\mathbb{Q}$. Suppose $f(x) = x^3 + ax^2 + bx + c$ is the minimal polynomial of x over $\mathbb{Q}$. Then the

roots of $f(x)$ are distinct, so the equation

$$y^2 = f(x)$$

defines an elliptic curve E over $\mathbb{Q}$. The two-torsion sugroup $E[2]$ of E over $\overline{\mathbb{Q}}$ consists of the points $\{(x_i, 0) : i = 1, 2, 3\} \cup \{\infty\}$ where x_1, x_2, x_3 are the roots of $f(x) = 0$. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the three non-identity elements of this group permutes them and gives the full group of permutations on three elements, since the Galois closure of F_3 over $\mathbb{Q}$ is an S_3-extension of $\mathbb{Q}$. Thus $E[2]$ is in fact isomorphic to the two-dimensional representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ over $k = \mathbb{Z}/2$ which is inflated from the representation V described above. Since N is contained in the maximal extension $\mathbb{Q}_{\{p\}}$ of $\mathbb{Q}$ which is unramified outside p, we see from this that the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[2]$ factors through $\mathrm{Gal}(\mathbb{Q}_{\{p\}}/\mathbb{Q}) = G$.

For simplicity, we will use V to denote the above representation of $\mathrm{Gal}(N/\mathbb{Q}) = S_4$ as well as the inflation of this representation to $\hat{S}_4 = \mathrm{Gal}(N'/\mathbb{Q})$ and to G. By Proposition 2.2 and Theorem 4.2, it follows that $R(G, V) \cong R(\mathrm{Gal}(N'/\mathbb{Q}), V)$ and that the image of the universal deformation $\rho : G \to \mathrm{GL}_2(R(G, V))$ is isomorphic to a quotient group of $\hat{S}_4 = \mathrm{Gal}(N'/\mathbb{Q})$.

Theorem 5.1. *Let p be as in Theorem 4.2. The universal deformation ring $R(\mathrm{Gal}(\mathbb{Q}_{\{p\}}/\mathbb{Q}), V) \cong R(\hat{S}_4, V)$ of V is isomorphic to $\mathbb{Z}_2[[t]]/(t^3 - 2t)$. In particular, $R(\mathrm{Gal}(\mathbb{Q}_{\{p\}}/\mathbb{Q}), V)$ is a complete intersection ring. Moreover, the image of the universal deformation $\rho : \mathrm{Gal}(\mathbb{Q}_{\{p\}}/\mathbb{Q}) \to \mathrm{GL}_2(R(\mathrm{Gal}(\mathbb{Q}_{\{p\}}/\mathbb{Q}), V))$ is isomorphic to $\hat{S}_4$.*

Proof. By [1, Theorem 2.3], when V is viewed as a module for S_4 over $k = \mathbb{Z}/2$, then $R(S_4, V) \cong \mathbb{Z}_2[[t]]/(t^2, 2t)$. In particular,

$$\mathrm{Ext}^1_{kS_4}(V, V) \cong \mathrm{Hom}_{\mathcal{C}}(R(S_4, V), k[\epsilon]/(\epsilon^2)) \cong k = \mathbb{Z}/2. \tag{5.1}$$

The double cover $\hat{S}_4$ is isomorphic to the binary octahedral group E_{48} of order 48, which can be written in terms of generators and relations as

$$E_{48} = \langle y, z \mid y^3 = z^4 = (yz)^2 = \omega,\ \omega^2 = 1 \rangle. \tag{5.2}$$

Moreover, E_{48} can be realized as the following subgroup of the real quaternions:

(5.3)
$$E_{48} = \left\{ \pm 1, \pm i, \pm j, \pm ij, \frac{\pm 1 \pm i \pm j \pm ij}{2} \right\} \cup \left\{ \frac{\pm u \pm v}{\sqrt{2}} \;\middle|\; u \neq v \text{ in } \{1, i, j, ij\} \right\}.$$

If we let $y = \frac{1+i+j+ij}{2}$ and $z = \frac{1+i}{\sqrt{2}}$, then y and z satisfy the relations in (5.2). We will identify $\hat{S}_4$ with E_{48} and S_4 with the quotient group $E_{48}/\langle\omega\rangle$.

Considering the ordinary character table of $\hat{S}_4$, we see that there are three ordinary irreducible representations of $\hat{S}_4$ of dimension 2. One of these representations is inflated from a representation of S_4, and thus equivalent to the representation $\varphi : \hat{S}_4 \to \mathrm{GL}_2(\mathbb{Z}_2)$ with

$$\varphi(y) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \qquad \varphi(z) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{5.4}$$

In particular, the reduction $\overline{\varphi}$ of φ mod 2 corresponds to V. The other two ordinary irreducible 2-dimensional representations ψ_1, ψ_2 of $\hat{S}_4$ are realizable over $\mathbb{Q}_2(\sqrt{2})$ and conjugate to each other under the action of the Galois group $\mathrm{Gal}(\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2)$.

If $\tau : \hat{S}_4 \to \mathrm{GL}_2(k[t]/(t^2))$ is a representation corresponding to an arbitrary lift of V over $k[t]/(t^2)$, then $\tau(z)$ is conjugate to a matrix of the form $T_z = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) + tA_z$ for a 2×2 matrix A_z with entries in $k = \mathbb{Z}/2$. But $(T_z)^4$ is the identity, which implies that $\tau(z)^4 = \tau(\omega)$ is the identity, and hence τ defines a representation of $S_4 = \hat{S}_4/\langle\omega\rangle$ over $k[t]/(t^2)$. It follows that the deformations of V, viewed as a $k\hat{S}_4$-module, over $k[t]/(t^2)$ are in bijection with the deformations of V, viewed as a kS_4-module, over $k[t]/(t^2)$. In particular, we obtain from (5.1) that

$$\mathrm{Ext}^1_{k\hat{S}_4}(V, V) \cong k = \mathbb{Z}/2, \tag{5.5}$$

and hence the universal mod 2 deformation ring $R(\hat{S}_4, V)/2R(\hat{S}_4, V)$ is a quotient of $k[[t]]$.

Let ξ be a square root of -15 in $\mathbb{Z}_2$. We get a representation Φ of $\hat{S}_4$ over $\mathbb{Z}_2$ defined by

(5.6)

$$\Phi(y) = \begin{pmatrix} 0 & -1 & -\frac{\xi-1}{\xi} & -\frac{3\xi+1}{2\xi} & -\frac{\xi+1}{2\xi} & -\frac{\xi-1}{2\xi} \\ 1 & -1 & \frac{3\xi-7}{2\xi} & -\frac{\xi+1}{\xi} & \frac{\xi-3}{2\xi} & -\frac{\xi-1}{2\xi} \\ 0 & 0 & \frac{\xi-3}{\xi} & \frac{\xi+2}{\xi} & -\frac{2}{\xi} & \frac{\xi+3}{2\xi} \\ 0 & 0 & -\frac{\xi-4}{\xi} & \frac{3}{\xi} & -\frac{\xi-1}{2\xi} & \frac{2}{\xi} \\ 0 & 0 & \frac{4}{\xi} & -\frac{\xi+3}{\xi} & \frac{\xi+5}{\xi} & -\frac{\xi+4}{\xi} \\ 0 & 0 & \frac{\xi-1}{\xi} & -\frac{4}{\xi} & \frac{\xi+2}{\xi} & -\frac{5}{\xi} \end{pmatrix}, \ \Phi(z) = \begin{pmatrix} 0 & 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & -2 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \end{pmatrix}.$$

This representation arises from a choice of $\mathbb{Z}_2$-lattice in the representation of $\hat{S}_4$ over $\mathbb{Q}_2$ whose character is equal to the sum of the absolutely irreducible characters of φ, ψ_1, ψ_2. Reducing Φ mod 2, we obtain a representation $\overline{\Phi}$ of $\hat{S}_4$ over k with

$$\overline{\Phi}(y) = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}, \qquad \overline{\Phi}(z) = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{5.7}$$

Let $\overline{U}$ be the corresponding $k\hat{S}_4$-module with k-basis $\{c_1, c_2, \ldots, c_6\}$. A linear algebra computation shows that the radical series of $\overline{U}$ is a composition series, which implies that $\overline{U}$ is a uniserial $k\hat{S}_4$-module. By using the endomorphism σ of $\overline{U}$ with $\sigma(c_a) = 0$ for $a = 1, 2$ and $\sigma(c_a) = c_{a-2}$ for $a = 3, 4, 5, 6$, we see that $\overline{U}$ provides a non-trivial lift of V over $k[t]/(t^3)$ as follows. Using as basis $\{c_5, \sigma c_5, \sigma^2 c_5, c_6, \sigma c_6, \sigma^2 c_6\}$, we can rewrite $\overline{\Phi}(y)$ and $\overline{\Phi}(z)$. Replacing σ by a variable t, we then get a representation $\overline{\rho} : \hat{S}_4 \to \mathrm{GL}_2(k[t]/(t^3))$ with

$$\overline{\rho}(y) = \begin{pmatrix} t^2 & 1 \\ 1 + t^2 & 1 \end{pmatrix}, \qquad \overline{\rho}(z) = \begin{pmatrix} t & 1 \\ 1 + t^2 & 0 \end{pmatrix} \tag{5.8}$$

which corresponds to the non-trivial lift of V over $k[t]/(t^3)$ defined by $\overline{U}$. Since $\overline{U}$ is indecomposable as a $k\hat{S}_4$-module, it follows that $\overline{\rho}$ is associated to a surjection from the universal mod 2 deformation ring of V onto $k[t]/(t^3)$.

Suppose the universal mod 2 deformation ring properly surjects onto $k[t]/(t^3)$. Then there is a lift of $\overline{\rho}$ over $k[t]/(t^4)$. Identifying $\overline{\rho}(y)$ (resp. $\overline{\rho}(z)$) with its natural preimage in $k[t]/(t^4)$, it follows that the representation corresponding to this lift is equivalent to a representation $\overline{\rho}_1$ with $\overline{\rho}_1(y) = \overline{\rho}(y) + t^3 B_y$ and $\overline{\rho}_1(z) = \overline{\rho}(z) + t^3 B_z$ for certain 2×2 matrices B_y, B_z with entries in $k = \mathbb{Z}/2$. Since $t^3 \cdot t^3 = 0$ in $k[t]/(t^4)$, we can use linear algebra to see that there are no matrices B_y, B_z such that $\overline{\rho}_1(y)$ and $\overline{\rho}_1(z)$ satisfy the relations in $\hat{S}_4$ modulo (t^4). Hence there is no lift of $\overline{\rho}$ over $k[t]/(t^4)$. By (5.5), this implies that the universal mod 2 deformation ring of V is $R(\hat{S}_4, V)/2R(\hat{S}_4, V) \cong k[t]/(t^3)$. Moreover, the representation $\overline{\rho}$ of $\hat{S}_4$ over $k[t]/(t^3)$ defines the universal mod 2 deformation of V.

To lift the endomorphism σ of $\overline{U}$ over $\mathbb{Z}_2$, we consider the conjugacy class of the element $z = \frac{1+i}{\sqrt{2}}$ of $\hat{S}_4$ of order 8. This conjugacy class has 6 elements:

$$z = \frac{1+i}{\sqrt{2}}, z^{-1} = \frac{1-i}{\sqrt{2}}, \frac{1+j}{\sqrt{2}}, \frac{1-j}{\sqrt{2}}, \frac{1+ij}{\sqrt{2}}, \frac{1-ij}{\sqrt{2}}.$$

Let K be the class sum of z. Then $\frac{1}{3}K$ is a central element of $\mathbb{Z}_2\hat{S}_4$. Hence $\Phi(\frac{1}{3}K)$ defines an endomorphism Σ of the representation Φ. We get that

$$\Sigma = \begin{pmatrix} 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & -2 & 0 & -2 & 0 \\ 0 & 0 & 0 & -2 & 0 & -2 \end{pmatrix}.$$

Then Σ has minimal polynomial $t^3 - 2t$. Using as basis $\{e_5, \Sigma e_5, \Sigma^2 e_5, e_6, \Sigma e_6, \Sigma^2 e_6\}$, we can rewrite $\Phi(y)$ and $\Phi(z)$. Replacing Σ by a variable t, we then get the representation ρ of $\hat{S}_4$ over $\mathbb{Z}_2[t]/(t^3 - 2t)$ given by

(5.9)

$$\rho(y) = \begin{pmatrix} -\frac{2t}{\xi} + \frac{(\xi+1)t^2}{2\xi} & -1 + \frac{(\xi+3)t}{2\xi} + \frac{(\xi-1)t^2}{2\xi} \\ 1 - \frac{(\xi-1)t}{2\xi} - \frac{(\xi-3)t^2}{2\xi} & -1 + \frac{2t}{\xi} + \frac{(\xi-1)t^2}{2\xi} \end{pmatrix}, \ \rho(z) = \begin{pmatrix} t & 1 \\ 1 - t^2 & 0 \end{pmatrix}.$$

The reduction of ρ mod 2 gives the representation $\overline{\rho}$ from (5.8) corresponding to the universal mod 2 deformation of V over $k[t]/(t^3)$. This means that $S = \mathbb{Z}_2[t]/(t^3 - 2t)$ is a quotient ring of $R(\hat{S}_4, V)$. Let $\alpha : R(\hat{S}_4, V) \to S$ be the corresponding surjective continuous $\mathbb{Z}_2$-algebra homomorphism. Then α induces an isomorphism $\overline{\alpha} : R(\hat{S}_4, V)/2R(\hat{S}_4, V) \to S/2S$. Since S is free over $\mathbb{Z}_2$, α splits when viewed as a $\mathbb{Z}_2$-module homomorphism. Hence this implies that α is an isomorphism and ρ defines the universal deformation of V over $S = \mathbb{Z}_2[t]/(t^3 - 2t)$. The matrices in (5.9) show that ρ is a faithful representation of $\hat{S}_4$, and hence its image is isomorphic to $\hat{S}_4$. □

References

1. F. M. Bleher and T. Chinburg, Universal deformation rings need not be complete intersections. Math. Ann. 337 (2007), no. 4, 739–767. MR2285736 (2008g:11093)
2. N. Boston, Galois p-groups unramified at p—a survey. Primes and knots, 31–40, Contemp. Math., 416, Amer. Math. Soc., Providence, RI, 2006. MR2276134 (2007k:11191)

3. N. Boston and R. Jones, Arboreal Galois representations. Geom. Dedicata 124 (2007), 27–35. MR2318536
4. G. Cornell, J. H. Silverman and G. Stevens (eds.), Modular Forms and Fermat's Last Theorem (Boston, MA, 1995). Springer-Verlag, Berlin-Heidelberg-New York, 1997. MR1638473 (99k:11004)
5. B. de Smit and H. W. Lenstra, Jr., Explicit construction of universal deformation rings. In: Modular Forms and Fermat's Last Theorem (Boston, MA, 1995), Springer-Verlag, Berlin-Heidelberg-New York, 1997, pp. 313–326. MR1638482
6. D. Gorenstein. Finite Groups, Harper and Row, New York, 1968. MR0231903 (38:229)
7. B. Mazur, Deforming Galois representations. In: Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), Springer-Verlag, Berlin-Heidelberg-New York, 1989, pp. 385–437. MR1012172 (90k:11057)
8. PARI2, PARI/GP, version 2.1.5, Bordeaux, 2004, `http://pari.math.u-bordeaux.fr/` and `ftp://megrez.math.u-bordeaux.fr/pub/numberfields/`.

Department of Mathematics, University of Iowa, Iowa City, Iowa 52242-1419
E-mail address: `fbleher@math.uiowa.edu`

Department of Mathematics, University of Pennsylvania, Philadelphia, Pennsylvania 19104-6395
E-mail address: `ted@math.upenn.edu`

Department of Mathematics, University of Iowa, Iowa City, Iowa 52242-1419
Current address: Department of Mathematics and Computer Science, Dickinson College, Carlisle, Pennsylvania 17013
E-mail address: `froelicj@dickinson.edu`