UNIVERSAL DEFORMATION RINGS NEED NOT BE COMPLETE INTERSECTIONS

FRAUKE M. BLEHER AND TED CHINBURG

ABSTRACT. We answer a question of M. Flach by showing that there is a linear representation of a profinite group whose (unrestricted) universal deformation ring is not a complete intersection. We show that such examples arise in arithmetic in the following way. There are infinitely many real quadratic fields F for which there is a mod 2 representation of the Galois group of the maximal unramified extension of F whose universal deformation ring is not a complete intersection. Finally, we discuss bounds on the singularities of universal deformation rings of representations of finite groups in terms of the nilpotency of the associated defect groups.

1. INTRODUCTION

In this article we provide an example of a representation of a profinite group whose unrestricted universal deformation ring is not a complete intersection, thus answering a question of M. Flach [9]. To our knowledge, this is the first example of such a representation. More precisely, we show the following Theorem.

Theorem 1.1. *Let k be a perfect field of characteristic $\ell = 2$.*

i. *There is a profinite group Γ and a simple $k\Gamma$-module V such that the universal deformation ring $R(\Gamma, V)$ is isomorphic to $W[[t]]/(2t, t^2)$, where $W = W(k)$ is the ring of infinite Witt vectors over k. In particular, $R(\Gamma, V)$ is not a complete intersection.*
ii. *There are infinitely many real quadratic fields F such that one can take the group Γ in part (i) to be $\mathrm{Gal}(F^{un}/F)$ when F^{un} is the maximal everywhere unramified extension of F.*

Flach's question arises naturally in number theory in the following way. 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. Mazur showed in [20], using results of Schlessinger, that under various hypotheses there are universal deformation rings $R_{\mathcal{D}}(G_{L,S}, V)$ associated to V and sets of deformation conditions $\mathcal{D}$. A key question in various applications, e.g. in the work of Wiles and Taylor in [25, 23], has been whether $R_{\mathcal{D}}(G_{L,S}, V)$ is a complete intersection ring. This has been shown to be true in many cases by a variety of authors when S contains all the places of L over ℓ and ∞. Most of these results involve deformation conditions $\mathcal{D}$ arising from the theory of modular forms; see [18], [12, 13] and their references. In [6], Böckle shows that the unrestricted universal deformation ring $R(G_{L,S}, V)$, with the empty set of deformation conditions $\mathcal{D}$, is a complete intersection in various arithmetic situations. In [10], de Jong replaces $G_{L,S}$ by the fundamental group $\pi_1(X)$ of a curve X in characteristic ℓ. He shows that under some mild hypotheses on V, $R(\pi_1(X), V)$ is a complete intersection if a counterpart of a conjecture of Deligne about geometric monodromy groups is true. He proves this counterpart when $n = 2$, and relates it in general to the Langlands correspondence mod ℓ. Further work along this line has been done by Gaitsgory in [15] and by Böckle and Khare in [7].

1991 *Mathematics Subject Classification.* Primary ; Secondary .
The first author was supported in part by NSF Grant DMS01-39737. The second author was supported in part by NSF Grant DMS00-70433.

It is not clear for which L, S and $\mathcal{D}$ the ring $R_{\mathcal{D}}(G_{L,S}, V)$ should be a complete intersection. A discussion of some expectations regarding the singularities of deformation rings is given in [19]. One expects that the addition of deformation conditions may in some cases eliminate singularities and may in other cases introduce them. Since Flach's question concerns the case in which $\mathcal{D}$ is empty, we will assume this from now on.

Suppose first that S contains all the places of L over ℓ and ∞ and where V ramifies. In [20], Mazur showed in case k finite that the Euler-Poincaré formula implies

$$\dim_k(\mathrm{H}^1(G_{L,S}, \mathrm{End}_k(V)) \geq \dim_k(\mathrm{H}^2(G_{L,S}, \mathrm{End}_k(V)).$$

This implies that the minimal number of generators in a presentation for $R(G_{L,S}, V)$ is at least as large as the number of relations. This is some evidence that $R(G_{L,S}, V)$ is often a complete intersection under the above hypotheses. Thus a natural extension of Flach's question would be to ask whether $R(G_{L,S}, V)$ is a complete intersection provided S contains all the places of L over ℓ and ∞ and where V ramifies.

The case in which S does not contain all the places of L over ℓ is fundamentally different. Suppose further that S contains no such places. By the Fontaine-Mazur conjecture, the image of $G_{L,S}$ under the universal deformation of V should be finite. The issue then becomes the study of universal deformations of finite groups, and there is less reason to expect the associated deformation rings to be complete intersections. In fact, Theorem 1.1(ii) produces infinitely many examples which are not complete intersections and for which L is real quadratic and $S = \emptyset$. Another point of view about the case in which S contains no place over ℓ is that the deformation theory of linear representations of $G_{L,S}$ does not provide a great deal of information about $G_{L,S}$. Boston has formulated a generalization of the Fontaine-Mazur conjecture (see [8]) which would provide much more information about pro-ℓ quotients of $G_{L,S}$ via actions of this group on rooted trees.

We recall now the definition of universal deformation rings. 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 [20] Mazur supposed V is absolutely irreducible, while in [11], 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.)

This paper is organized in the following way. In §2 we prove Theorem 1.1(i) when Γ is the symmetric group S_4 on 4 letters and V is two-dimensional and irreducible; this V is unique up to isomorphism. The proof relies on results of the first author in [1], and the method used can be applied to more complicated representations of finite groups.

To produce number theoretic examples, we introduce in §3 the notion of capping groups. A surjection $\pi : \Gamma \to G$ of profinite groups shows that G caps Γ for a prime ℓ if $\mathrm{Ker}(\pi)$ has no non-trivial pro-ℓ quotients (c.f. Definition 3.1). We show that under this condition, the versal deformation rings of all mod ℓ representations of G do not change under inflation from G to Γ. In Lemma 3.3 we show that this property in fact characterizes when G caps Γ for ℓ via $\pi : \Gamma \to G$. The notion of capping groups arises naturally in Iwasawa theory, e.g. it can be used to define when a rational prime ℓ is regular (c.f. Proposition 3.6). In §4 we analyze which groups are capped by S_4 for $\ell = 2$.

To apply this to the Galois groups $G_{L,S}$ discussed above, it is useful to know when $G_{L,S}$ can be capped for a given prime ℓ by a finite quotient G of $G_{L,S}$. In §5 we show that when $L = \mathbb{Q}$, $\ell = 2$ and G is a symmetric group S_n, then there is an S for which $G_{L,S}$ is capped by S_n if and only if $n = 2$ or $n = 3$. When one enlarges the base field L to a real quadratic field, however, we show in §6 that S_4 caps $G_{L,\emptyset}$ for infinitely many real quadratic fields L. This is shown by first exhibiting explicitly one field L and by then applying a Cebotarev argument. This leads to the result in Theorem 1.1(ii).

In the last section §7 of this paper we consider the following question:

Question 1.2. *Suppose k is a field of characteristic $\ell > 0$, G is a finite group and that V is a kG-module of finite dimension over k which belongs to a block B of kG having a defect group D which has nilpotency r. Suppose further that the stable endomorphism ring $\underline{\mathrm{End}}_{kG}(V)$ of V is one-dimensional over k, so that $R(G,V)$ is well defined. Is it the case that $\dim(R(G,V)) - \mathrm{depth}(R(G,V)) \leq r-1$?*

Note that if $R(G,V)$ is Cohen-Macaulay (e.g. if $R(G,V)$ is a complete intersection), then $\dim(R(G,V)) = \mathrm{depth}(R(G,V))$, so this question has an affirmative answer. We show that Question 1.2 has an affirmative answer in various other cases using results from [20], [3], [1] and [2].

We would like to thank M. Flach for letting us know about his question concerning whether all universal deformation rings are complete intersections. We would like to thank the referee for some very useful comments improving the paper.

Some of the results of this paper have been announced in [5].

2. The non-trivial irreducible mod 2 representation of S_4

Let k be a perfect field of characteristic 2 and let S_4 denote the symmetric group on 4 letters. Up to isomorphism, there is a unique non-trivial irreducible kS_4-module V, and $\dim_k V = 2$. In this section, we prove that the universal deformation ring of V is not a complete intersection ring. We use the following Lemma, which is a correction of [1, Lemma 4.1].

Lemma 2.1. *Let k be a perfect field of characteristic 2, and let W be the ring of infinite Witt vectors over k. Let R be a complete local Noetherian W-algebra for which there is a continuous surjection $\tau : R \to W$ and an isomorphism $\mu : R/2R \to k[s]/(s^2)$ of W-algebras. Then R is isomorphic to $W[[t]]/(t^2 - 2\gamma t, \alpha 2^m t)$ as a W-algebra, where $\gamma \in W$, $\alpha \in \{0,1\}$ and $0 < m \in \mathbb{Z}$. In particular, R is isomorphic to a subquotient algebra of the group ring $W(\mathbb{Z}/2\mathbb{Z})$ of $\mathbb{Z}/2\mathbb{Z}$ or to a quotient algebra of $W[t]/(t^2)$. If moreover there is exactly one continuous surjection τ, then either $\gamma = 0$ or $\alpha = 1$.*

Proof. It follows from the assumptions that there is a continuous W-algebra surjection $\psi : W[[t]] \to R$. By composing ψ with the automorphism of $W[[t]]$ which sends t to $t - a$ for $a = \tau(\psi(t)) \in W$, we can assume that $\tau(\psi(t)) = 0$. This means that the kernel J of ψ is contained in the ideal (t), and, since $R/2R \cong k[s]/(s^2)$, J is properly contained in (t). Since the maximal ideal of $W[[t]]$ is generated by 2 and t, the maximal ideal of $R/2R$ is generated by the image of t. Because $R/2R \cong k[s]/(s^2)$, we conclude that the image of $W \oplus Wt \subset W[[t]]$ under $\psi : W[[t]] \to R$ must be all of R since R is complete. Hence $\psi(t^2) = \psi(a_0 + a_1 t)$ for some $a_0, a_1 \in W$, which means that $t^2 - (a_0 + a_1 t) = j \in J$. Since J is a proper subset of (t), it follows that $a_0 = 0$ and a_1 is not a unit in W, i.e. $a_1 = 2\gamma$ for some $\gamma \in W$. Therefore, $(t^2 - 2\gamma t)W[[t]] \subseteq J \subset tW[[t]]$. Hence $J = tJ'$ where $(t - 2\gamma)W[[t]] \subseteq J' \subset W[[t]]$, and the latter inclusion is proper since $J \neq tW[[t]]$. It follows that $J' = (t - 2\gamma, \alpha 2^m)$ where $\alpha \in \{0,1\}$ and $m \in \mathbb{Z}^+$. Thus $J = (t^2 - \gamma t, \alpha 2^m t)$.

If $\gamma = 0$, $R \cong W[[t]]/(t^2, \alpha 2^m t)$ is isomorphic to a quotient algebra of $W[[t]]/(t^2) \cong W[t]/(t^2)$. If $\gamma \neq 0$, $R \cong W[[t]]/(t^2 - 2\gamma t, \alpha 2^m t)$ is isomorphic to a quotient algebra of $W[[t]]/(t^2 - 2\gamma t)$. There is an injective W-algebra homomorphism

$$\rho : W[[t]]/(t(t - 2\gamma)) \to W \times W$$

which sends t to $(0, 2\gamma)$. Thus the image of ρ is $\{(x,y) \in W \times W \mid x \equiv y \mod 2\gamma W\}$ which is a W-subalgebra of $\{(x,y) \in W \times W \mid x \equiv y \mod 2W\} \cong W(\mathbb{Z}/2\mathbb{Z})$. If $\gamma \neq 0$ and $\alpha \neq 1$, then $R \cong W[[t]]/(t(t - 2\gamma))$ has two continuous surjections onto W. □

Remark 2.2. Let R be a commutative local Noetherian ring. Grothendieck [16, §19.3] calls R a complete intersection ring if there is a regular complete local commutative Noetherian ring S and a regular sequence $x_1, \dots, x_n \in S$ such that the completion $\hat{R}$ is isomorphic to $S/(x_1, \dots, x_n)$.

Suppose that B is a regular commutative local Noetherian ring, and J is an ideal of B. By [16, Prop. (19.3.2)], it follows that $A = B/J$ is a complete intersection ring if and only if the ideal J is generated by a regular sequence of elements in B.

Theorem 2.3. *Let k be a perfect field of characteristic 2, let W be the ring of infinite Witt vectors over k, and let S_4 be the symmetric group on 4 letters. Let V be a non-trivial irreducible kS_4-module of dimension 2. Then the universal deformation ring of V is $R(S_4, V) \cong W[[t]]/(t^2, 2t)$. In particular, $R(S_4, V)$ is not a complete intersection ring.*

Proof. By [1, Proof of Prop. 4.2], there is exactly one continuous surjective W-algebra homomorphism $R = R(S_4, V) \to W$, and $R/2R \cong k[t]/(t^2)$. By Lemma 2.1, R is isomorphic to $W[[t]]/(t^2 - 2\gamma t, \alpha 2^m t)$, where $\gamma \in W$, $\alpha \in \{0, 1\}$, $0 < m \in \mathbb{Z}$ and either $\gamma = 0$ or $\alpha = 1$. Let $G = \langle u, v, r, s \mid \mathrm{Rel} \rangle$ with

$$\mathrm{Rel} = \{u^2 = v^2 = r^3 = s^2 = 1, uv = vu, srs = r^{-1}, sus = v, svs = u, rur^{-1} = v, rvr^{-1} = uv\}.$$

By letting $u = (1,2)(3,4)$, $v = (1,4)(2,3)$, $r = (1,2,3)$ and $s = (1,3)$, we see that G is isomorphic to S_4. The representation $\overline{\rho} : S_4 \to \mathrm{GL}_2(k)$ corresponding to V is given by the following matrices

$$\overline{\rho}(u) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \overline{\rho}(v), \quad \overline{\rho}(r) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad \overline{\rho}(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{2.1}$$

We now construct a representation $\tau : G = S_4 \to \mathrm{GL}_2(W[[t]]/(t^2, 2t))$ which mod 2 gives a universal mod 2 deformation of V. Define τ by the following matrices:

$$\tau(u) = \begin{pmatrix} 1+t & t \\ 0 & 1+t \end{pmatrix}, \ \tau(v) = \begin{pmatrix} 1+t & 0 \\ t & 1+t \end{pmatrix}, \ \tau(r) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \ \tau(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The reduction $\overline{\tau}$ of τ mod 2 defines an indecomposable kS_4-module $\overline{U}$ satisfying $t\overline{U} \cong V$ and $\overline{U}/t\overline{U} \cong V$. It follows from $R(S_4, V)/2R(S_4, V) \cong k[t]/(t^2)$ that $\overline{U}$ is isomorphic to the universal mod 2 deformation of V as kS_4-module. The reduction of τ mod (t) defines a deformation of V over W and corresponds to the unique surjection $R(S_4, V) \to W = R(S_3, V)$ mentioned earlier.

Suppose now that R is not isomorphic to $W[[t]]/(t^2, 2t)$, i.e. $R = W[[z]]/(z^2 - 2\gamma z, \alpha 2^m z)$ so that if $\alpha = 1$ then $m \geq 2$. Recall $\gamma = 0$ or $\alpha = 1$. To obtain a contradiction, we need to show there are no γ and α as above such that τ can be lifted to $W[[z]]/(z^2 - 2\gamma z, \alpha 2^m z)$ via a continuous W-algebra homomorphism

$$\nu : R = W[[z]]/(z^2 - 2\gamma z, \alpha 2^m z) \to W[[t]]/(t^2, 2t)$$

which induces an isomorphism $R/2R \to k[t]/(t^2)$. One checks that $\nu(z) = \kappa t$ for some $\kappa \in W^*$, so on replacing γ by $\kappa^{-1}\gamma$ we can reduce to the case in which $\nu(z) = t$. Since $W[[t]]/(t^2 - 2\gamma t, 4t)$ is a quotient algebra of $W[[z]]/(z^2 - 2\gamma z, \alpha 2^m z)$ through which ν factors, it is enough to show that τ cannot be lifted to $W[[t]]/(t^2 - 2\gamma t, 4t)$ for any $\gamma \in W$ for the canonical projection $\pi_\gamma : W[[t]]/(t^2 - 2\gamma t, 4t) \to W[[t]]/(t^2, 2t)$ sending t to t.

This can be seen by looking at $\tau(u)$. If $\hat{\tau}$ were a lift of τ to $W[[t]]/(t^2 - 2\gamma t, 4t)$ for π_γ, then $\hat{\tau}(u)$ would be conjugate to a matrix A_u over $W[[t]]/(t^2 - 2\gamma t, 4t)$ which has to satisfy the relation $A_u^2 \equiv I \bmod (t^2 - 2\gamma t, 4t)$, where I denotes the identity 2×2 matrix. An easy matrix calculation shows that this is not possible. Hence τ cannot be lifted to $W[[t]]/(t^2 - 2\gamma t, 4t)$ for any $\gamma \in W$, which implies that $R = R(S_4, V) \cong W[[t]]/(t^2, 2t)$. □

Remark 2.4. Theorem 2.3 provides a correction of [1, Prop. 4.2]. However, $R(S_4, V)$ is still isomorphic to a subquotient ring of WD_8. This follows, since $R(S_4, V)$ is a quotient algebra of $W[t]/(t^2)$ by Theorem 2.3, and it was shown in the proof of [1, Cor. 4.3] that $W[t]/(t^2)$ is isomorphic to a subquotient ring of WD_8. Hence [1, Cor. 4.3] is still correct, i.e. if X is a simple kS_4-module, then $R(S_4, X)$ is a subquotient ring of the group ring WD over W of a defect group D of the block B of kS_4 associated to X.

3. Capping groups

In this section we introduce the notion of capping groups. One application of this concept is to the computation of the universal or versal deformation ring of a mod ℓ representation of a profinite group.

Definition 3.1. Let ℓ be a prime number, and suppose there is a short exact sequence

$$1 \to K \to \Gamma \xrightarrow{\pi} G \to 1 \tag{3.1}$$

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.

Remark 3.2. Let ℓ, Γ, G, π and K be as in Definition 3.1.

i. The following are equivalent:
   a. The group G caps Γ via π for ℓ.
   b. The pro-ℓ completion of K is trivial.
   c. The maximal pro-ℓ abelian quotient of K is trivial.
   d. The maximal ℓ-elementary abelian quotient of K (which may be infinitely generated) is trivial.
   e. There is no closed normal subgroup K' of K with the property that K/K' is a non-trivial pro-ℓ group.

ii. If G caps Γ via π for ℓ, then for all closed subgroups H of G, H caps $\pi^{-1}(H)$ for ℓ.

iii. Let G^{ab} (resp. Γ^{ab}) be the maximal pro-abelian quotient group of G (resp. Γ). If G caps Γ via π for ℓ, then G^{ab} caps Γ^{ab} for ℓ.

We now relate the concept of capping groups to deformation theory. For simplicity, we suppose that Γ satisfies the following ℓ-finiteness condition of Mazur [20]: For every continuous finite-dimensional $k\Gamma$-module X, the k-dimension of $\mathrm{H}^1(\Gamma, X)$ is finite. By [20], this implies that if V is a continuous finite-dimensional representation of Γ over a discrete perfect field k of characteristic ℓ, the versal deformation ring $R(\Gamma, V)$ is well defined.

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, 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.

Proof. The fact that (i) implies (ii) follows since the kernel of the natural surjection

$$\mathrm{Aut}_{R(\Gamma,V)}(U(\Gamma, V)) \to \mathrm{Aut}_k(V)$$

is a pro-ℓ group.

We now assume (ii) and suppose that G does not cap Γ via π for ℓ. We may thus suppose that there is a closed normal subgroup K_0 of Γ contained in K such that K/K_0 is a non-trivial pro-ℓ group. Since Γ/K_0 is a pro-finite group, there is an open normal subgroup K' of finite index in Γ with the following property. The exact sequence

$$1 \to K/(K \cap K_0) \to \Gamma/K_0 \to G/\pi(K_0) \to 1$$

gives an exact sequence

$$1 \to K/(K \cap (K'K_0)) \to \Gamma/(K'K_0) \to G/\pi(K'K_0) \to 1$$

in which $K/(K \cap (K'K_0))$ is a non-trivial finite ℓ-group. Here $\Gamma/(K'K_0)$ is a finite group. By Theorem 3.2 of [4], there is a finite dimensional representation V of $\Gamma/(K'K_0)$ over k which is inflated from a representation of $G/\pi(K'K_0)$ such that the versal deformation $U(\Gamma/(K'K_0), V)$ is faithful.

In particular, the group $K/(K \cap (K'K_0))$ acts non-trivially on $U(\Gamma/(K'K_0), V)$. We now inflate this V from $\Gamma/(K'K_0)$ to Γ. Since $U(\Gamma/(K'K_0), V)$ must arise from the versal deformation $U(\Gamma, V)$ of V as a representation of Γ, we see that K acts non-trivially on $U(\Gamma, V)$ because $K/(K \cap (K'K_0))$ acts non-trivially on $U(\Gamma/(K'K_0), V)$. This completes the proof. □

Definition 3.4. 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 (3.1) 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 $G_{L,S}$ for ℓ.
iii. We say G *is a capping group* for ℓ if G caps some number field L for ℓ.

The natural question in this context is:

Question 3.5. *Given a prime ℓ, which profinite groups G are capping groups for ℓ? Which of these cap $\mathbb{Q}$ for ℓ?*

We give one example of how one can phrase statements in Iwasawa theory in terms of capping groups.

Proposition 3.6. *Suppose ℓ is an odd prime.*

i. *The field $\mathbb{Q}(\zeta_{\ell^\infty})^+$ is the unique extension of $\mathbb{Q}$ which is unramified outside $\{\ell\}$ and with Galois group $G = \mathbb{Z}_\ell^*/\{\pm 1\}$.*
ii. *The group G caps $\mathbb{Q}$ for ℓ at $S = \{\ell\}$ if and only if the maximal abelian pro-ℓ extension of $\mathbb{Q}(\zeta_{\ell^\infty})^+$ which is unramified outside $\{\ell\}$ is trivial. This holds if and only if ℓ is regular in the sense that ℓ does not divide the class number of $\mathbb{Q}(\zeta_\ell)$.*

Proof. Part (i) follows from classical cyclotomic theory. Hence the canonical continuous surjection

$$\pi : G_{\mathbb{Q},S} \to G$$

is unique up to an automorphism of G.

By [24, Thm. 5.34 and Prop. 13.22], ℓ is regular if and only if the minus part of the class number of $\mathbb{Q}(\zeta_{\ell^n})$ is not divisible by ℓ for all $n \geq 1$. By [24, Prop. 13.32], this is equivalent to the maximal abelian outside ℓ unramified pro-ℓ extension of $\mathbb{Q}(\zeta_{\ell^\infty})^+$ being trivial. This is so if and only if G caps $\mathbb{Q}$ (via π) for ℓ. □

Our main result on capping groups is the following theorem.

Theorem 3.7. *Let S_n denote the symmetric group on n letters.*

i. *The group S_n caps $\mathbb{Q}$ for $\ell = 2$ if $n = 2, 3$ and does not cap $\mathbb{Q}$ for $\ell = 2$ if $n \geq 4$.*
ii. *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.*

Remark 3.8. A group G caps a number field L for ℓ at a set S of places of L if and only if there is a G-extension L' of L which is unramified outside S satisfying the following. For all conductors $\mathcal{M}$ in L' which involve only places lying over S, the ray class group of L' of conductor $\mathcal{M}$ has order prime to ℓ. In particular, part (ii) in Theorem 3.7 is equivalent to the statement that there are infinitely many real quadratic fields L for which there is an unramified S_4-extension of L which has odd class number. An example of such a field is $L = \mathbb{Q}(\sqrt{5 \cdot 14197})$.

As a corollary of Theorem 2.3 and Theorem 3.7, we obtain the following result which implies Theorem 1.1.

Corollary 3.9. *Let k be a perfect field of characteristic 2, and let V be a non-trivial irreducible kS_4-module of dimension 2. There are infinitely many real quadratic fields L such that*

i. *There is surjection $\pi : G_{L,\emptyset} \to S_4$, and*

ii. *When V is viewed as a module for $G_{L,\emptyset}$ via π, then*

$$R(G_{L,\emptyset}, V) = R(S_4, V) \cong W[[t]]/(t^2, 2t)$$

is not a complete intersection ring.

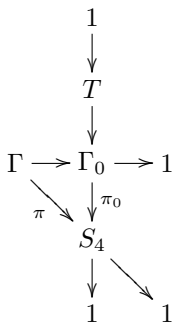
4. Groups capped by S_4 for $\ell = 2$

Lemma 4.1. *Suppose there is a short exact sequence*

$$1 \to K \to \Gamma \xrightarrow{\pi} S_4 \to 1$$

where Γ is a profinite group, π is a continuous group homomorphism and K is a closed normal subgroup of Γ. Then S_4 caps Γ via π for $\ell = 2$ if and only if there is no commutative diagram with exact rows and columns

(4.1)



where either $T \cong \mathbb{Z}/2$ with trivial S_4-action, or $T \cong V$ where $V = \mathbb{Z}/2 \times \mathbb{Z}/2$ and the action of S_4 on V is given by the same matrices as in (2.1).

Proof. Suppose that S_4 does not cap Γ for $\ell = 2$. Since S_4 is finite, this implies that there is a closed normal subgroup $K_0 \leq K$ of Γ such that $T = K/K_0$ is a finite 2-group. We have a short exact sequence

$$1 \to T = K/K_0 \to \Gamma/K_0 \to \Gamma/K = S_4 \to 1. \tag{4.2}$$

We can replace T by $T^{\mathrm{ab}}/(T^{\mathrm{ab}})^2$ so as to be able to assume that T is an elementary abelian 2-group. Since S_4 acts on T by conjugation, T is a $(\mathbb{Z}/2)S_4$-module. Since every irreducible $(\mathbb{Z}/2)S_4$-module is isomorphic to either the trivial simple module $\mathbb{Z}/2$ or to the non-trivial simple module V, we can replace T by a quotient so as to be able to assume that T is either $\mathbb{Z}/2$ or V. Setting $\Gamma_0 = \Gamma/K_0$ in (4.2) results in a diagram (4.1). □

The following two Lemmas analyze the group Γ_0 in diagram (4.1) if it exists.

Lemma 4.2. *Suppose that there is a group Γ_0 as in diagram* (4.1) *in which $T = \mathbb{Z}/2$ with trivial action by S_4. Then one of the following mutually exclusive possibilities occurs:*

a. *There is a surjection of Γ_0 onto a group of order* 4.
b. *There is an embedding $\rho : \Gamma_0 \to \mathrm{GL}_2(\mathbb{C})$ which gives a lifting of a faithful projective representation $\tilde{\rho} : S_4 = \Gamma_0/T \to \mathrm{PGL}_2(\mathbb{C})$ in the sense of Tate and Serre* [22, §6]. *This leads to two isomorphism classes of Γ_0 which can be distinguished by $\det(\rho)$ having order* 1 *or* 2.

In both cases, if S_3 is a subgroup of S_4 isomorphic to the symmetric group on 3 *letters then the maximal abelian quotient of $\pi_0^{-1}(S_3)$ has order* 4.

Proof. The description of the groups in parts (a) and (b) is well-known and can easily be proved by computing $\mathrm{H}^2(S_4, \mu_2)$ using the Kummer sequence

$$1 \to \mu_2 \to \mathbb{C}^* \xrightarrow{z \to z^2} \mathbb{C}^* \to 1.$$

In both cases, we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{Z}/2 & \longrightarrow & \Gamma_0 & \xrightarrow{\pi} & S_4 & \longrightarrow & 1 \\ & & \| & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \mathbb{Z}/2 & \longrightarrow & \pi_0^{-1}(S_3) & \longrightarrow & S_3 & \longrightarrow & 1 \end{array}$$

where the vertical arrows are inclusions. Since $\pi_0^{-1}(S_3)$ is not isomorphic to A_4, $\pi_0^{-1}(S_3)$ has a normal Sylow 3-subgroup P_3. Since $\pi_0^{-1}(S_3)$ is not abelian, this means that the maximal abelian quotient of $\pi_0^{-1}(S_3)$ has order 4. □

Lemma 4.3. *Suppose that there is a group Γ_0 as in diagram (4.1) in which $T \cong V = \mathbb{Z}/2 \times \mathbb{Z}/2$ with the action of S_4 on V being given by the matrices in (2.1). Then Γ_0 is a semidirect product $\Gamma_0 = H \rtimes S_3$ where either*

a. *$H \cong V \oplus V \cong (\mathbb{Z}/2)^4$; or*
b. *$H \cong \mathbb{Z}/4 \times \mathbb{Z}/4$.*

In both cases, if D_8 is a Sylow 2-subgroup of S_4, so that D_8 is isomorphic to a dihedral group of order 8, then the maximal abelian quotient of $\pi_0^{-1}(D_8)$ has order 8.

Proof. Since $\mathrm{H}^2(S_4, V)$ has 2 elements, there are precisely two possibilities for Γ_0, up to isomorphism. This leads to the description of Γ_0 as $\Gamma_0 = H \rtimes S_3$ where H is as in part (a) or (b).

In both cases (a) and (b), there is an exact sequence

$$1 \to M \to \pi_0^{-1}(D_8) \to \mathbb{Z}/2 = \{1, \sigma\} \to 1$$

where M is isomorphic to $(\mathbb{Z}/2)\{1, \sigma\} \oplus (\mathbb{Z}/2)\{1, \sigma\}$ (resp. to $(\mathbb{Z}/4)\{1, \sigma\}$) as a module for the group $\{1, \sigma\}$ under the conjugation action of σ in case (a) (resp. in case (b)). In either case, $(1-\sigma)M$ is an order 4 subgroup of M which is stable under the left action of σ, where the action of σ corresponds to conjugation by a pre-image of σ in $\pi_0^{-1}(D_8)$. It follows that $(1-\sigma)M$ is a normal subgroup of $\pi_0^{-1}(D_8)$ and $\pi_0^{-1}(D_8)/(1-\sigma)M$ is abelian of order 8. Since the commutator subgroup of $\pi_0^{-1}(D_8)$ has non-trivial intersection with $T \cong V$ and since there is also a non-trivial element in the commutator subgroup of $\pi_0^{-1}(D_8)/T \cong S_4$, it follows that the maximal abelian quotient of $\pi_0^{-1}(D_8)$ has order at most $32/4 = 8$. This completes the proof of Lemma 4.3. □

5. S_n-extensions of $\mathbb{Q}$

Our goal in this section is to show that S_n caps $\mathbb{Q}$ for $\ell = 2$ for $n = 2, 3$ and not for any $n \geq 4$, which proves part (i) of Theorem 3.7.

We first dispense with the cases $n = 2$ and $n = 3$.

Lemma 5.1. *If $n = 2$, the group $S_2 \cong \mathbb{Z}/2$ caps $\mathbb{Q}$ for $\ell = 2$ at $S = \{5\}$ via any $\pi : G_{\mathbb{Q},S} \to S_2$. If $n = 3$, the group S_3 caps $\mathbb{Q}$ for $\ell = 2$ at $S = \{23, \infty\}$ via any $\pi : G_{\mathbb{Q},S} \to S_3$.*

Proof. When $n = 2$, it follows from class field theory that the field $\mathbb{Q}(\sqrt{5})$ is the maximal pro-2 extension of $\mathbb{Q}$ which is unramified outside $\{5\}$. When $n = 3$, one finds similarly that the splitting field N of $f(x) = x^3 - x - 1$ is a the unique S_3-extension of $\mathbb{Q}$ unramified outside $\{23, \infty\}$, and this field has no extension of two-power degree unramified outside $\{23, \infty\}$. □

We now recall some results from [22, §6] concerning liftings of projective representations of $G_L = \mathrm{Gal}(\overline{L}/L)$ when L is a global or local field.

Suppose

$$\tilde{\rho} : G_L \to \mathrm{PGL}_m(\mathbb{C})$$

is an m-dimensional projective representation. A lifting of $\tilde{\rho}$ is a continuous linear representation

$$\rho : G_L \to \mathrm{GL}_m(\mathbb{C})$$

giving rise to $\tilde{\rho}$ via the canonical surjection $\mathrm{GL}_m(\mathbb{C}) \to \mathrm{PGL}_m(\mathbb{C})$. If ρ is such a lifting, then all other liftings have the form $\chi \otimes \rho$ for some one-dimensional character χ of G_L.

Suppose v is a place of L. Let $\overline{v}$ be a place of $\overline{L}$ over v, and define $I_{L,v} \subset D_{L,v} \subset G_L$ to be the inertia and decomposition groups of $\overline{v}$. These groups are determined by v up to conjugation.

Theorem 5.2. (Tate) *For all global and local fields L, the cohomology group $\mathrm{H}^2(G_L, \mathbb{C}^*)$ is trivial. In consequence, every projective representation of G_L has a lifting.*

Theorem 5.3. (Tate) *Suppose that $L = \mathbb{Q}$ and that $\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}_m(\mathbb{C})$ is a projective representation. For each prime number p, let $\rho'_p : D_{\mathbb{Q},p} \to \mathrm{GL}_m(\mathbb{C})$ be a lifting of the restriction $\tilde{\rho}|D_{\mathbb{Q},p}$ of $\tilde{\rho}$ to $D_{\mathbb{Q},p}$. Suppose that $\rho'_p|I_{\mathbb{Q},p}$ is trivial for almost all p. Then there is a unique lifting ρ of $\tilde{\rho}$ such that*

$$\rho|I_{\mathbb{Q},p} = \rho'_p|I_{\mathbb{Q},p} \tag{5.1}$$

for all primes p.

It is important to note that this Theorem specifies the restriction of a lifting to the inertia groups of finite places of $\mathbb{Q}$, not on the decomposition groups of these places. Further, the Theorem does not specify the lifting on the inertia group at infinity.

The following result can easily be proved by considering the S_n-cohomology of the Kummer sequence $1 \to \{\pm 1\} \to \mathbb{C}^* \to \mathbb{C}^* \to 1$.

Lemma 5.4. *For $n \geq 4$, there is an embedding of S_n into $\mathrm{PGL}_m(\mathbb{C})$ for some m which does not lift to an embedding of S_n into $\mathrm{GL}_m(\mathbb{C})$.*

Proof of part (i) of Theorem 3.7.
By Lemma 5.1, the Theorem is true for $n = 2, 3$. Suppose now that $n \geq 4$. Let S be a finite set of places of $\mathbb{Q}$, and let $G_{\mathbb{Q},S}$ be the Galois group of the maximal unramified outside S extension of $\mathbb{Q}$. Suppose $\pi : G_{\mathbb{Q},S} \to S_n$ is a surjection. Let $\mathbb{Q}_S$ be the maximal unramified outside S extension of $\mathbb{Q}$. Then $N = \mathbb{Q}_S^{\mathrm{Ker}(\pi)}$ is an S_n-extension of $\mathbb{Q}$ unramified outside S. Our goal is to show that S_n does not cap $G_{\mathbb{Q},S}$ via π for $\ell = 2$. This is equivalent to showing that there is a Galois extension N' of N such that $\mathrm{Gal}(N'/N)$ is a non-trivial pro-2 group and $N' \subset \mathbb{Q}_S$. If S contains the prime 2, then the composition of N with the cyclotomic totally real $\mathbb{Z}_2$-extension of $\mathbb{Q}$ is such a field N'. So in what follows, we assume that S does not contain 2.

By Lemma 5.4, there is an embedding ι of S_n into $\mathrm{PGL}_m(\mathbb{C})$ for some m which does not lift to an embedding of S_n into $\mathrm{GL}_m(\mathbb{C})$. The composition of the natural surjection $G_{\mathbb{Q}} \to G_{\mathbb{Q},S}$ with π followed by ι gives a projective representation

$$\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}_m(\mathbb{C})$$

which is unramified outside S. By Theorem 5.2 applied to the completions of $\mathbb{Q}$, there is a lifting ρ'_p of the restriction of $\tilde{\rho}$ to $D_{\mathbb{Q},p}$ for all primes p. If p is unramified, the image of $\tilde{\rho}|D_{\mathbb{Q},p}$ is cyclic, and we can assume ρ'_p is unramified. Theorem 5.3 now shows that there is a lifting

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_m(\mathbb{C})$$

of $\tilde{\rho}$ for which (5.1) is true. In particular, ρ is unramified outside of $S \cup \{\infty\}$.

Suppose S does not contain the real place ∞ of $\mathbb{Q}$, and that ρ is ramified at ∞. Then N must be totally real, and if c is a complex conjugation in $G_{\mathbb{Q}}$, $\rho(c)$ is the negative $-I$ of the $m \times m$ identity matrix I. Since S does not contain 2, the quadratic subfield F of N must be unramified over 2. Let p be an (odd) prime ramifying in F. Then there is a character χ_p of $(\mathbb{Z}/p)^*$ such that $\chi_p(-1) = -1$. View χ_p as a character of $G_{\mathbb{Q}}$ which is unramfied outside of p and ∞. Then $\chi_p \otimes \rho$ is unramified outside S, since $\chi_p(c) \cdot \rho(c) = I$. Thus on replacing ρ by $\chi_p \otimes \rho$, we can assume ρ is unramified outside S in all cases.

The image Θ of ρ is a central extension of $S_n = \tilde{\rho}(G_{\mathbb{Q}}) = \mathrm{Gal}(N/\mathbb{Q})$ by a finite cyclic group $\mu_r = \rho(\mathrm{Ker}(\tilde{\rho})) \subset \mathbb{C}^* \cdot I$. Thus Θ defines an extension class in $\mathrm{H}^2(S_n, \mu_r)$ whose image in $\mathrm{H}^2(S_n, \mathbb{C}^*) \cong \mathbb{Z}/2$ is the unique non-trivial class. Thus r must be even. Let N'' be the extension $\mathbb{Q}_S^{\mathrm{Ker}(\rho)}$, and let N'

be the quadratic extension of N given by $(N'')^{\mu_{r/2}}$, where $\mu_{r/2}$ is the unique subgroup of index 2 in $\mu_r \subset \Theta$. Then N'/N is a degree two extension which is unramified outside S, which shows that S_n does not cap $G_{\mathbb{Q},S}$ via $\pi : G_{\mathbb{Q},S} \to S_n = \mathrm{Gal}(N/\mathbb{Q})$ for $\ell = 2$. This completes the proof of part (i) of Theorem 3.7.

The following result will be used in §6 to prove part (ii) of Theorem 3.7.

Lemma 5.5. *Suppose $p \equiv 1 \mod 4$ and $\tilde{\rho} : G_{\mathbb{Q},\{p\}} \to \mathrm{PGL}_2(\mathbb{C})$ has image isomorphic to S_4.*

i. *There exist precisely two non-isomorphic liftings $\rho' : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{C})$ of $\tilde{\rho}$ with $\det(\rho') = 1$. They differ by twisting with the one-dimensional character given by the quadratic residue symbol $\left(\frac{*}{p}\right)$, and each has $\#\mathrm{Image}(\rho') = 48$.*

ii. *Suppose now that $p \equiv 5 \mod 8$. There exist precisely two non-isomorphic liftings $\rho : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{C})$ of $\tilde{\rho}$ which are unramified outside p and such that $\#\mathrm{Image}(\rho) = 48$. Fix a lifting $\rho' : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{C})$ of $\tilde{\rho}$ with $\det(\rho') = 1$ as in part (i). Let ξ be one of the two Dirichlet characters of conductor p and order 4. Then $\rho = \eta \otimes \rho'$ for a one-dimensional character η specified by the following conditions.*

   a. *If ρ' is unramified at ∞ then $\eta \in \{\mathrm{id}, \xi^2\}$ and $\det(\rho)$ is trivial.*

   b. *If ρ' is ramified at ∞ then $\eta \in \{\xi, \xi^{-1}\}$ and $\det(\rho) = \xi^2 = \left(\frac{*}{p}\right)$ has order 2.*

iii. *In either of case ii(a) or ii(b), the fixed field $N' = \mathbb{Q}_{\{p,\infty\}}^{\mathrm{Ker}(\rho)}$ does not depend on the choice of η, and is a quadratic extension of $N = \mathbb{Q}_{\{p\}}^{\mathrm{Ker}(\tilde{\rho})}$. In case ii(a) (resp. ii(b)), every prime of N over p is quadratically ramified in N' (resp. is unramified in N').*

Proof. Throughout the proof we assume that $\tilde{\rho}$ is given by $\tilde{\rho} : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{PGL}_2(\mathbb{C})$ which factors through $G_{\mathbb{Q},\{p\}}$.

By Tate's Theorems 5.2 and 5.3, there is a lifting $\rho' : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{C})$ of $\tilde{\rho}$. Let c be a complex conjugation in $G_{\mathbb{Q},\{p,\infty\}}$. Then $\tilde{\rho}(c)$ equals the identity element, since $\tilde{\rho}$ factors through $G_{\mathbb{Q},\{p\}}$. Hence $\rho'(c)$ must be $\pm I$ when I is the identity matrix. The one-dimensional characters χ of $G_{\mathbb{Q},\{p,\infty\}}$ correspond to Dirichlet characters of conductor p, and there is such a χ for which $\chi(c) \cdot I = \rho'(c)$. Then $\chi \otimes \rho'$ is not ramified at infinity, so $\det(\chi \otimes \rho') = \chi^2 \det(\rho')$ is a one-dimensional character which is unramified outside p. In particular, this character is not ramified at infinity, so it corresponds to a character of $(\mathbb{Z}/p)^*$ which is trivial on -1. This implies $\det(\chi \otimes \rho') = \chi'^2$ for some character χ'. On replacing the lift ρ' by $\chi'^{-1} \otimes \chi \otimes \rho'$ we obtain $\det(\rho') = 1$. The restriction of ρ' to $\mathrm{Ker}(\tilde{\rho})$ must have image in the scalar matrices, and must be non-trivial since there is no lifting of $S_4 \subset \mathrm{PGL}_2(\mathbb{C})$ to an isomorphic subgroup of $\mathrm{GL}_2(\mathbb{C})$. Hence $\det(\rho') = 1$ implies $\rho'(\mathrm{Ker}(\tilde{\rho}))$ consists of $\{\pm I\}$, and $\#\mathrm{Image}(\rho') = 48$.

Suppose ρ_0 is another lifting of $\tilde{\rho}$ with $\det(\rho_0) = 1$. Then $\rho_0 = \chi'' \otimes \rho'$ for some one-dimensional character χ'' of $G_{\mathbb{Q},\{p,\infty\}}$. Since $\det(\rho_0) = \chi''^2 = 1$, it follows that χ'' is given by the quadratic residue symbol $\left(\frac{*}{p}\right)$. To finish the proof of part (i) we need to show that ρ' and $\left(\frac{*}{p}\right) \otimes \rho'$ are not isomorphic. Fix an isomorphism of $\tilde{\rho}(G_{\mathbb{Q},\{p\}})$ with S_4. The composition of this isomorphism with the sign character of S_4 is a quadratic character of $G_{\mathbb{Q},\{p\}}$, which must correspond to $\left(\frac{*}{p}\right)$. Hence to show that ρ' and $\left(\frac{*}{p}\right) \otimes \rho'$ are not isomorphic, it will suffice to show that any element $g \in G_{\mathbb{Q},\{p,\infty\}}$ which maps to a cycle of order 4 in $\tilde{\rho}(G_{\mathbb{Q},\{p\}}) \cong S_4$ must have $\mathrm{Tr}(\rho'(g)) \neq 0$. If $\mathrm{Tr}(\rho'(g)) = 0$, then the eigenvalues of $\rho'(g)$ would be λ and $-\lambda$ for some $\lambda \in \mathbb{C}^*$. But then $\rho'(g^2)$ would a scalar matrix since it is semi-simple, contradicting the fact that $\tilde{\rho}(g^2)$ is not the identity.

To prove part (ii), we assume $p \equiv 5 \bmod 8$ and we fix a lifting $\rho' : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{C})$ of $\tilde{\rho}$ with $\det(\rho') = 1$. All other lifts of $\tilde{\rho}$ as a representation of $G_{\mathbb{Q},\{p,\infty\}}$ have the form $\rho = \eta \otimes \rho'$ for a one-dimensional character η of $G_{\mathbb{Q},\{p,\infty\}}$. We first determine necessary and sufficient conditions on η for $\#\mathrm{Image}(\rho) = 48$.

The arguments of part (i) show that the restriction of ρ to $\mathrm{Ker}(\tilde{\rho})$ is non-trivial and has image in $\mathbb{C}^* \cdot I$. It follows that $\#\mathrm{Image}(\rho) = 48$ if and only if $\det(\rho) = \det(\rho') \cdot \eta^2 = \eta^2$ has trivial restriction

to $\mathrm{Ker}(\tilde{\rho})$. This is true if and only if η^2 is either the trivial abelian character or the inflation of the sign character of $\mathrm{Image}(\tilde{\rho}) \cong S_4$, the latter character corresponding to $\left(\frac{*}{p}\right)$. This is equivalent to the statement that $\eta \in \{\mathrm{id}, \xi, \xi^2, \xi^3\}$ when ξ is either one of the two order four characters of conductor p.

Suppose now that $\eta \in \{\mathrm{id}, \xi, \xi^2, \xi^3\}$. We consider the further condition that ρ be unramified outside p, so that it is inflated from a representation of $G_{\mathbb{Q},\{p\}}$. This will be so exactly when $\rho(c) = \eta(c) \cdot \rho'(c) = I$ when c is a complex conjugation, or equivalently when $\rho'(c) = \eta(c)^{-1} \cdot I$. Since $p \equiv 5 \bmod 8$, we have $\xi(c) = -1$. This together with $\rho'(c) = \pm I$, $\eta \in \{\mathrm{id}, \xi, \xi^2, \xi^3\}$ and $\det(\rho) = \det(\rho') \cdot \eta^2 = \eta^2$ leads to statements (a) and (b) of part (ii). The fact that the two twists involved in either (a) or (b) are distinct can be proved by the argument used in part (i).

To show part (iii), note that in either of the two cases in part (ii), the field $N' = \mathbb{Q}_{\{p,\infty\}}^{\mathrm{Ker}(\rho)}$ does not depend on the choice of η, since ξ^2 is trivial on $\mathrm{Ker}(\tilde{\rho})$. When $N = \mathbb{Q}_{\{p,\infty\}}^{\mathrm{Ker}(\tilde{\rho})}$, the extension $N/\mathbb{Q}$ is an S_4 extension and $[N' : N] = 2$. Let $I_p \subset G_{\mathbb{Q},\{p,\infty\}}$ be an inertia group at p. The group $\tilde{\rho}(I_p)$ has even order since $\mathbb{Q}(\sqrt{p}) = N^{A_4}$ is quadratically ramified at p. Since $p \equiv 5 \bmod 8$, p must be tamely ramified in N and N', so $\tilde{\rho}(I_p)$ and $\rho'(I_p)$ are cyclic. It follows that $\tilde{\rho}(I_p) \subset S_4$ is cyclic of order 2 or 4, while $\rho'(I_p)$ is cyclic of order 2, 4 or 8. Since $\det(\rho') = 1$, there is a one-dimensional character ψ of I_p of order dividing 8 such that $\rho'|I_p \cong \psi \oplus \psi^{-1}$. The fact that $p \equiv 5 \bmod 8$ means that ψ cannot have order 8. The order of ψ cannot divide 2 since this would imply that $\tilde{\rho}(I_p)$ would be trivial. Hence ψ has order 4 and corresponds to either ξ or ξ^{-1}. Thus if $\rho = \rho'$ or $\rho = \xi^2 \otimes \rho'$ as in case (a) of part (ii), we get that $\rho|I_p \cong \xi \oplus \xi^{-1}$. In this case, $\rho(I_p)$ has order 4 while $\tilde{\rho}(I_p)$ has order 2, so every prime over p in N ramifies in N'. In case (b) of part (ii), we find that $\rho|I_p = 1 \oplus \xi^2$, so $\rho(I_p)$ and $\tilde{\rho}(I_p)$ both have order 2 and no prime of N over p ramifies in N'. □

6. S_4-extensions of real quadratic fields

The object of this section is to prove the following Theorem which implies part (ii) of Theorem 3.7 and Corollary 3.9.

Theorem 6.1. *There are infinitely many pairs (p, q) of distinct odd primes with the following property. There is an everywhere unramified S_4-extension N' of $\mathbb{Q}(\sqrt{pq})$ which has odd class number. Let $\pi : G_{\mathbb{Q}(\sqrt{pq}),\emptyset} \to \mathrm{Gal}(N'/\mathbb{Q}(\sqrt{pq})) = S_4$ be the associated surjection. Then S_4 caps $G_{\mathbb{Q}(\sqrt{pq}),\emptyset}$ via π for $\ell = 2$. Let V be the inflation to $G_{\mathbb{Q}(\sqrt{pq}),\emptyset}$ of the non-trivial irreducible two-dimensional representation of S_4 over a perfect field k of characteristic 2. Then the universal deformation ring $R(G_{\mathbb{Q}(\sqrt{pq}),\emptyset}, V)$ is isomorphic to $W[[t]]/(t^2, 2t)$ and is not a complete intersection ring.*

To begin the proof, we start by analyzing certain S_4-extensions of $\mathbb{Q}$.

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 $p \equiv 1 \bmod 4$. 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 1 primes.*

Proof. The extension $N/\mathbb{Q}$ is unramified outside of p, and $G = \mathrm{Gal}(N/\mathbb{Q})$ is a subgroup of S_4 of order divisible by 4. Let $\mathfrak{I}(G, \mathcal{P})$ be the inertia group in G of a prime $\mathcal{P}$ over p in N. The conjugates of $\mathfrak{I}(G, \mathcal{P})$ generate G since $\mathbb{Q}$ has no non-trivial finite extension. A Sylow 2-subgroup of $\mathfrak{I}(G, \mathcal{P})$ is cyclic and non-trivial since $p > 2$. This implies that either $G \cong \mathbb{Z}/4 = \mathfrak{I}(G, \mathcal{P})$, or $G = S_4$. But $G \cong \mathbb{Z}/4$ is impossible since the discriminant of F_4 over $\mathbb{Q}$ is p. Since the quadratic subfield F_2 of N is real and unramified outside p, we conclude that $F_2 = \mathbb{Q}(\sqrt{p})$ with $p \equiv 1 \bmod 4$.

The possible ways that p can split in F_4 are (i) $(p) = \mathcal{P}_1^2\mathcal{P}_2\mathcal{P}_3$, where the $\mathcal{P}_i$ are degree one primes; or (ii) $(p) = \mathcal{P}_1^2\mathcal{P}_2$ in which $\mathcal{P}_1$ has degree 1 and $\mathcal{P}_2$ has degree 2. Suppose that (ii) occurs. Then the decomposition group $\mathfrak{D}(G, \mathcal{P})$ of a prime $\mathcal{P}$ over p in N has order 4, while the inertia

group $\mathfrak{I}(G,\mathcal{P})$ has order 2. Since $\mathcal{P}_2$ ramifies in N, $\mathfrak{I}(G,\mathcal{P})$ intersects $\mathrm{Gal}(N/F_4) \cong S_3$ non-trivially, so $\mathfrak{I}(G,\mathcal{P})$ contains a transposition. This implies $\mathfrak{D}(G,\mathcal{P})$ is a non-cyclic group of order 4 which is not normal in $G = \mathrm{Gal}(N/\mathbb{Q}) \cong S_4$. Let $\tilde{\rho} : G \to \mathrm{PGL}_2(\mathbb{C})$ be a projective embedding of G. By Lemma 5.5(i), there exists a lifting $\rho' : \mathrm{Gal}(\mathbb{Q}_{\{p,\infty\}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ of $\tilde{\rho}$ such that $\det(\rho') = 1$. This implies that if $\sigma \in \mathrm{Gal}(\mathbb{Q}_{\{p,\infty\}}/N)$ then $\rho'(\sigma)$ must be $\pm I$ since $\rho'(\sigma)$ is a scalar matrix with determinant 1. Thus if $\tilde{N} = \mathbb{Q}_{\{p,\infty\}}^{\mathrm{Ker}(\rho')}$, the group $\Gamma_0 = \mathrm{Gal}(\tilde{N}/\mathbb{Q})$ is isomorphic via ρ' to a subgroup of $\mathrm{GL}_2(\mathbb{C})$, and the natural map $\mathrm{GL}_2(\mathbb{C}) \to \mathrm{PGL}_2(\mathbb{C})$ leads to an exact sequence

$$0 \to \mathrm{Gal}(\tilde{N}/N) \to \Gamma_0 \to G \to 0 \tag{6.1}$$

in which $H = \mathrm{Gal}(\tilde{N}/N)$ has order 1 or 2. In fact, H must have order 2, since $G = S_4$ has no faithful representation in $\mathrm{GL}_2(\mathbb{C})$. Let $I_p \subset D_p \subset G_{\mathbb{Q},\{p,\infty\}}$ be an inertia and decomposition group at p. Then $\rho'(D_p)$ is an extension of $\mathfrak{D}(G,\mathcal{P}) \cong (\mathbb{Z}/2) \times (\mathbb{Z}/2)$ by a group of order 1 or 2. On the other hand, $\rho'(D_p)$ is a finite 2-group quotient of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ and is thus a 2-group quotient of $\langle s,t | sts^{-1} = t^p \rangle$ such that the image of $\langle t \rangle$ is the ramification subgroup. Since $\rho'(I_p)$ has order divisible by 4 and since we assume $p \equiv 1 \bmod 4$, the group $\rho'(D_p)$ is isomorphic to a quotient of the abelian group $\mathbb{Z} \times (\mathbb{Z}/4)$, and hence to a quotient of $(\mathbb{Z}/2) \times (\mathbb{Z}/4)$. Since $\det(\rho')$ is trivial and neither $(\mathbb{Z}/2) \times (\mathbb{Z}/2)$ nor $(\mathbb{Z}/2) \times (\mathbb{Z}/4)$ have a faithful two-dimensional complex representation with trivial determinant, we get a contradiction. This proves p splits in F_4 as $\mathcal{P}_1^2\mathcal{P}_2\mathcal{P}_3$ with each $\mathcal{P}_i$ of degree 1.

We see from $\mathrm{Gal}(N/F_4) \cong S_3$ that the inertia group of a prime over p in N is of order 2 and is generated by a transposition. The residue field degree of a prime over p in N is one, since $\mathcal{P}_1$, $\mathcal{P}_2$ and $\mathcal{P}_3$ have degree 1 and N is the compositum of the conjugates of F_4. Hence the inertia and decomposition groups of a prime over p are the same. Finally, one has $(p) = \mathcal{Q}_1^2\mathcal{Q}_2$ in F_3 with $\mathcal{Q}_i$ of degree 1 because $\mathrm{Gal}(N/F_3)$ is a Sylow 2-subgroup of $\mathrm{Gal}(N/\mathbb{Q})$, which contains some but not all of the inertia groups of primes over p in N. □

Lemma 6.3. *Let N be as in Proposition 6.2, and suppose that $p \equiv 5 \bmod 8$. 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 $k(\mathcal{P}_3)$.

Proof. Suppose first that N'/N is a quadratic extension having the properties stated in the second sentence of the Lemma. Then $\mathrm{Gal}(N'/\mathbb{Q})$ must be one of the groups described in Lemma 4.2. In case (a) of Lemma 4.2, there would be an abelian extension of $\mathbb{Q}$ of degree 4 contained in N'. This extension would be unramified outside $\{p\}$ and totally real. However, the hypothesis that $p \equiv 5 \bmod 8$ means that there is no such extension, since the Sylow 2-subgroup of $(\mathbb{Z}/p)^*/\{\pm 1\}$ has order 2. So $\mathrm{Gal}(N'/\mathbb{Q})$ has to be as in case (b) of Lemma 4.2, and N' must be associated to a lifting of $\tilde{\rho}$.

The remaining assertions in the Lemma follow directly from Lemma 5.5 except for the final statement about case (b). We now assume that case (b) occurs. By Lemma 4.2, there is a field L such that $F_4 \subset L \subset N'$ and L/F_4 is an abelian extension of degree 4. Recall that $(p) = \mathcal{P}_1^2\mathcal{P}_2\mathcal{P}_3$ in F_4, and that all primes over p are quadratically ramified in N. Since N'/N is unramified, $\mathcal{P}_1$ does not ramify in the extension L/F_4, and $\mathcal{P}_2$ and $\mathcal{P}_3$ can be at most quadratically ramified. Consider the (surjective) Artin map

$$\psi : Cl_{\mathcal{P}_2\mathcal{P}_3}(F_4) \to \mathrm{Gal}(L/F_4) \tag{6.2}$$

where $Cl_{\mathcal{P}_2\mathcal{P}_3}(F_4)$ is the ray class group. We have an exact sequence

$$1 \to \frac{k(\mathcal{P}_2)^* \times k(\mathcal{P}_3)^*}{\text{Image}(O_{F_4}^*)} \to Cl_{\mathcal{P}_2\mathcal{P}_3}(F_4) \to Cl(F_4) \to 1 \tag{6.3}$$

where $Cl(F_4)$ is the class group of F_4 and $O_{F_4}^*$ is mapped diagonally into the residue fields of $\mathcal{P}_2$ and $\mathcal{P}_3$. The map ψ in (6.2) must be trivial on $k(\mathcal{P}_2)^{*2} \times k(\mathcal{P}_3)^{*2}$ since L/F_4 is at most quadratically ramified at $\mathcal{P}_2$ and $\mathcal{P}_3$. The group

$$\frac{\left(\frac{k(\mathcal{P}_2)^*}{k(\mathcal{P}_2)^{*2}}\right) \times \left(\frac{k(\mathcal{P}_3)^*}{k(\mathcal{P}_3)^{*2}}\right)}{\text{Image}(O_{F_4}^*)}$$

has order 4 if and only if every unit in $O_{F_4}^*$ is a square in $k(\mathcal{P}_2)^*$ and in $k(\mathcal{P}_3)^*$; otherwise it has order 1 or 2. Thus from (6.3) and the fact that L/F_4 has degree 4, we conclude that either $\#Cl(F_4)$ is even, or every unit in $O_{F_4}^*$ is a square in $k(\mathcal{P}_2)^*$ and in $k(\mathcal{P}_3)^*$. □

We now assume $p \equiv 5 \bmod 8$, and pick an auxiliary prime r satisfying the following hypotheses:

Hypothesis 6.4. Let r be a rational prime such that:

a. $r \equiv 1 \bmod 4$.
b. the quadratic residue symbol $\left(\frac{p}{r}\right) = -1$. Equivalently, p is a non-square mod r, and by quadratic reciprocity, r is a non-square mod p.

We are going to analyze the restriction of a lifting ρ satisfying the hypotheses of Lemma 6.3 to $G_{\mathbb{Q}(\sqrt{pr})}$. To do this, we first need to prove some results about $\mathbb{Q}(\sqrt{pr})$.

Lemma 6.5. *The narrow class numbers $h^+_{\mathbb{Q}(\sqrt{p})}$ and $h^+_{\mathbb{Q}(\sqrt{r})}$ are odd, and the fundamental units of $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{r})$ have norm -1 to $\mathbb{Q}$. The class number $h_{\mathbb{Q}(\sqrt{pr})}$ is exactly divisible by 2. The maximal abelian two-extension of $\mathbb{Q}(\sqrt{pr})$ which is unramified over $\mathbb{Q}(\sqrt{pr})$ is $\mathbb{Q}(\sqrt{p},\sqrt{r})$. Let $\mathcal{P}$ be the unique prime over p in $\mathbb{Q}(\sqrt{pr})$, so that $(p) = \mathcal{P}^2$ as ideals of $O_{\mathbb{Q}(\sqrt{pr})}$. The order of the Sylow 2-subgroup of the ray class group $Cl_{\mathcal{P}}(\mathbb{Q}(\sqrt{pr}))$ is 2, so the natural surjection*

$$Cl_{\mathcal{P}}(\mathbb{Q}(\sqrt{pr})) \to Cl(\mathbb{Q}(\sqrt{pr}))$$

is an isomorphism on Sylow 2-subgroups. There are no characters of $Cl_{\mathcal{P}}(\mathbb{Q}(\sqrt{pr}))$ which quadratically ramify at $\mathcal{P}$.

Proof. By classical genus theory, $h^+_{\mathbb{Q}(\sqrt{p})}$ and $h^+_{\mathbb{Q}(\sqrt{r})}$ are odd, and a fundamental unit in each of these fields has norm -1 to $\mathbb{Q}$.

Since the quadratic residue symbol $\left(\frac{p}{r}\right) = -1$, p is inert in $\mathbb{Q}(\sqrt{r})$. Consider the ray classgroup $Cl_{(p)}(\mathbb{Q}(\sqrt{r}))$. Since $h^+_{\mathbb{Q}(\sqrt{r})}$ is odd, so is the class number $h_{\mathbb{Q}(\sqrt{r})}$. Hence the Sylow 2-subgroup of $Cl_{(p)}(\mathbb{Q}(\sqrt{r}))$ is isomorphic to the Sylow 2-subgroup of

$$\frac{k((p))^*}{\text{Image}(O^*_{\mathbb{Q}(\sqrt{r})})} \tag{6.4}$$

where $k((p))$ is the residue field of the ideal (p) of $O_{\mathbb{Q}(\sqrt{r})}$. Since p is inert in $\mathbb{Q}(\sqrt{r})$, the order of $k((p))$ is p^2. Here $p \equiv 5 \bmod 8$ implies that $p^2 \equiv 5^2 = 25 \bmod 16$, so that $8||\#k((p))^* = p^2 - 1$.

Let ϵ_r be a fundamental unit of $\mathbb{Q}(\sqrt{r})$. Since p is inert in $\mathbb{Q}(\sqrt{r})$, the Frobenius automorphism of $k((p))$ is the map $\alpha \to \alpha^p$, and this corresponds to the non-trivial element σ of $\text{Gal}(\mathbb{Q}(\sqrt{r})/\mathbb{Q})$. Since we have shown ϵ_r has norm -1 to $\mathbb{Q}$, we have

$$-1 = \text{Norm}_{\mathbb{Q}(\sqrt{r})/\mathbb{Q}}(\epsilon_r) = \epsilon_r^{1+\sigma} = \epsilon_r^{1+p} \quad \text{in} \quad k((p))^*. \tag{6.5}$$

Now $8||p^2 - 1 = \#k((p))^*$ means that the Sylow 2-subgroup of $k((p))^*$ is cyclic of order 8, and $-1 = \epsilon_r^{1+p}$ is the element of order 2 in this group. Since $2||(1+p) \equiv 6 \bmod 8$, we see that the projection of ϵ_r to the Sylow 2-subgroup of $k((p))^*$ has to have order exactly 4.

Since -1 is a square in $k((p))^*$ and $8||\#k((p))^*$, we conclude that the Sylow 2-subgroup of (6.4) has order exactly two. Thus the Sylow 2-subgroup of $Cl_{(p)}(\mathbb{Q}(\sqrt{r}))$ has order exactly 2. Since $\mathbb{Q}(\sqrt{p},\sqrt{r})/\mathbb{Q}(\sqrt{r})$ is an abelian two-extension which is ramified only at (p), this field must be the maximal abelian two-extension of $\mathbb{Q}(\sqrt{r})$ which is unramified outside $\{(p)\}$.

If $\mathbb{Q}(\sqrt{p},\sqrt{r})$ had even class number, then by considering the maximal quotient of the two-part of the class group of $\mathbb{Q}(\sqrt{p},\sqrt{r})$ on which $\mathrm{Gal}(\mathbb{Q}(\sqrt{p},\sqrt{r})/\mathbb{Q}(\sqrt{r}))$ acts trivially, we would produce a non-trivial two-extension L of $\mathbb{Q}(\sqrt{p},\sqrt{r})$ which is abelian over $\mathbb{Q}(\sqrt{r})$ and unramified over $\mathbb{Q}(\sqrt{p},\sqrt{r})$. However, $L/\mathbb{Q}(\sqrt{r})$ would then be an abelian two-extension of order at least 4 which is unramified outside of (p), contradicting the fact that the Sylow 2-subgroup of $Cl_{(p)}(\mathbb{Q}(\sqrt{r}))$ has order exactly 2. Thus $\mathbb{Q}(\sqrt{p},\sqrt{r})$ must have odd class number. Since $\mathbb{Q}(\sqrt{p},\sqrt{r})$ is an unramified quadratic extension of $\mathbb{Q}(\sqrt{pr})$, this forces $2||h_{\mathbb{Q}(\sqrt{pr})}$, and $\mathbb{Q}(\sqrt{p},\sqrt{r})$ is the two-Hilbert classfield of $\mathbb{Q}(\sqrt{pr})$.

It remains to show that the order of the Sylow 2-subgroup of the ray class group $Cl_{\mathcal{P}}(\mathbb{Q}(\sqrt{pr}))$ is 2 when $\mathcal{P}$ is the unique prime over p in $\mathbb{Q}(\sqrt{pr})$. Here we have an exact sequence

$$1 \to \frac{k(\mathcal{P})^*}{\mathrm{Image}(O^*_{\mathbb{Q}(\sqrt{pr})})} \to Cl_{\mathcal{P}}(\mathbb{Q}(\sqrt{pr})) \to Cl(\mathbb{Q}(\sqrt{pr})) \to 1 \tag{6.6}$$

in which the Sylow 2-subgroup of $Cl(\mathbb{Q}(\sqrt{pr}))$ has order 2 and $k(\mathcal{P})^*$ is cyclic. Suppose the Sylow 2-subgroup of $Cl_{\mathcal{P}}(\mathbb{Q}(\sqrt{pr}))$ has order at least 4. Let H be the subgroup of $Cl_{\mathcal{P}}(\mathbb{Q}(\sqrt{pr}))$ generated by the image of $k(\mathcal{P})^{*2}$ in (6.6) together with the Sylow l-subgroups of $Cl_{\mathcal{P}}(\mathbb{Q}(\sqrt{pr}))$ as l ranges over all odd primes. Since $\mathcal{P}$ is stable under $\mathrm{Gal}(\mathbb{Q}(\sqrt{pr})/\mathbb{Q})$, and the Sylow l-subgroups of $Cl_{\mathcal{P}}(\mathbb{Q}(\sqrt{pr}))$ are unique, we conclude that H is stable under the action of $\mathrm{Gal}(\mathbb{Q}(\sqrt{pr})/\mathbb{Q})$. Now $Cl_{\mathcal{P}}(\mathbb{Q}(\sqrt{pr}))/H$ has order 4, and corresponds to an extension L of $\mathbb{Q}(\sqrt{pr})$ which is abelian of order 4, at most quadratically ramified at $\mathcal{P}$ and unramified elsewhere, and Galois over $\mathbb{Q}$ since H was stable under the action of $\mathrm{Gal}(\mathbb{Q}(\sqrt{pr})/\mathbb{Q})$. This L contains $\mathbb{Q}(\sqrt{p},\sqrt{r})$, since we have shown $\mathbb{Q}(\sqrt{p},\sqrt{r})$ is the 2-Hilbert class field of $\mathbb{Q}(\sqrt{pr})$. Since L is a Galois extension of $\mathbb{Q}$ of degree 8, and $\mathbb{Q}(\sqrt{r}) \subset \mathbb{Q}(\sqrt{r},\sqrt{p}) \subset L$, we conclude that $L/\mathbb{Q}(\sqrt{r})$ is Galois of degree 4. Thus L is an abelian extension of $\mathbb{Q}(\sqrt{r})$ of degree 4. Now r is quadratically ramified in L, since it quadratically ramifies in $\mathbb{Q}(\sqrt{pr})$ and $L/\mathbb{Q}(\sqrt{pr})$ is unramified outside $\{\mathcal{P}\}$. Furthermore, $L/\mathbb{Q}$ is unramified outside $\{p,r\}$. Since r is already quadratically ramified in $\mathbb{Q}(\sqrt{r})$, we conclude that $L/\mathbb{Q}(\sqrt{r})$ is an abelian quartic extension which is unramified outside of the unique prime (p) over p in $\mathbb{Q}(\sqrt{r})$. This forces the Sylow 2-subgroup of the ray class group $Cl_{(p)}(\mathbb{Q}(\sqrt{r}))$ to have order at least 4, which is a contradiction. We conclude that no field L of the above kind exists, so the order of the Sylow 2-subgroup of the ray class group $Cl_{\mathcal{P}}(\mathbb{Q}(\sqrt{pr}))$ is 2. This means that the natural homomorphism

$$Cl_{\mathcal{P}}(\mathbb{Q}(\sqrt{pr})) \to Cl(\mathbb{Q}(\sqrt{pr})) \tag{6.7}$$

is an isomorphism on Sylow 2-subgroups. If there were a character χ of $Cl_{\mathcal{P}}(\mathbb{Q}(\sqrt{pr}))$ which quadratically ramifies at $\mathcal{P}$, we could take an odd power of this character to have a character of two-power order of $Cl_{\mathcal{P}}(\mathbb{Q}(\sqrt{pr}))$ which does not factor through $Cl(\mathbb{Q}(\sqrt{pr}))$. This contradicts the fact that (6.7) is an isomorphism on Sylow 2-subgroups, so the proof of Lemma 6.5 is complete. □

Proposition 6.6. *Suppose that $p \equiv 5 \mod 8$ and $r \equiv 1 \mod 4$ are primes for which the following is true:*

a. *There is a quartic field F_4 with the properties listed in Proposition 6.2. The class number h_{F_4} is odd, and there is a unit in $O^*_{F_4}$ which is not a square in at least one of $k(\mathcal{P}_2)^*$ or $k(\mathcal{P}_3)^*$, where as in Proposition 6.2, $(p) = \mathcal{P}_1^2\mathcal{P}_2\mathcal{P}_3$ in F_4.*
b. $\left(\frac{r}{p}\right) = -1$.
c. *As in Proposition 6.2, let F_3 be one of the cubic subfields of the Galois closure N of F_4 over $\mathbb{Q}$. The class number of the field $F_3(\sqrt{r})$ is exactly divisible by 2.*

Then the field $N(\sqrt{pr})$ is an unramified S_4-extension of $\mathbb{Q}(\sqrt{pr})$ which has odd class number.

Proof. By Proposition 6.2, p is quadratically ramified in N and $N/\mathbb{Q}$ is unramified outside of p. Since p is odd, if L_1 and L_2 are quadratic extensions of $\mathbb{Q}_p$ which are ramified, then L_1L_2 is unramified over L_1. It follows that since p is quadratically ramified in $\mathbb{Q}(\sqrt{pr})$, the field $N(\sqrt{pr})$ is unramified over $\mathbb{Q}(\sqrt{pr})$. Because $r \neq p$ and $\mathbb{Q}(\sqrt{p})$ is the unique quadratic subfield of N, the fields N and $\mathbb{Q}(\sqrt{pr})$ are linearly disjoint over $\mathbb{Q}$. Hence $\mathrm{Gal}(N(\sqrt{pr})/\mathbb{Q}(\sqrt{pr}))$ is isomorphic to $S_4 = \mathrm{Gal}(N/\mathbb{Q})$ and

$$\mathrm{Gal}(N(\sqrt{pr})/\mathbb{Q}) \cong \mathrm{Gal}(N/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{pr})/\mathbb{Q}) \cong S_4 \times \mathbb{Z}/2.$$

The simple $\mathbb{Z}/2$-modules with an action of $S_4 \times \mathbb{Z}/2$ are the module $\mathbb{Z}/2$ with trivial action and the inflation V to $S_4 \times \mathbb{Z}/2$ of the two-dimensional irreducible representation of S_4 over $\mathbb{Z}/2$ given by the matrices in (2.1).

Suppose that the Sylow 2-subgroup of the ideal class group of $N(\sqrt{pr})$ is non-trivial. Consider a composition series for this Sylow 2-subgroup as a module for the group ring of $\mathrm{Gal}(N(\sqrt{pr})/\mathbb{Q})$ over $\mathbb{Z}/2$. From the above description of the simple modules for $\mathrm{Gal}(N(\sqrt{pr})/\mathbb{Q})$ over $\mathbb{Z}/2$ we conclude that there is a Galois extension L of $N(\sqrt{pr})$ with the following properties. The extension $L/\mathbb{Q}$ is Galois. The group $T = \mathrm{Gal}(L/N(\sqrt{pr}))$ is either $\mathbb{Z}/2$ with trivial action by $\mathrm{Gal}(N(\sqrt{pr})/\mathbb{Q})$ or the simple module $V = \mathbb{Z}/2 \times \mathbb{Z}/2$ for $\mathrm{Gal}(N(\sqrt{pr})/\mathbb{Q})$ which is described above.

Suppose first that $T = \mathbb{Z}/2$ with trivial action by $\mathrm{Gal}(N(\sqrt{pr})/\mathbb{Q})$. We have an exact sequence

$$1 \to T \to \mathrm{Gal}(L/\mathbb{Q}(\sqrt{pr})) \to \mathrm{Gal}(N(\sqrt{pr}))/\mathbb{Q}(\sqrt{pr})) \to 1.$$

Thus $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{pr})$ must be one of the groups considered in Lemma 4.2. In case (a) of Lemma 4.2, there would have to be a quartic abelian extension F of $\mathbb{Q}(\sqrt{pr})$ which is contained in L. Because $L/\mathbb{Q}(\sqrt{pr})$ is unramified, this would imply that the class number of $\mathbb{Q}(\sqrt{pr})$ is divisible by 4, which is not the case by Lemma 6.5. Thus $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{pr}))$ is one of the groups appearing in case (b) of Lemma 4.2.

Let

$$\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{C})$$

be a projective representation which factors through a faithful projective representation of $\mathrm{Gal}(N/\mathbb{Q})$ into $\mathrm{PGL}_2(\mathbb{C})$, as in Lemma 6.3. Let $\tilde{\rho}_{pr}$ be the restriction of $\tilde{\rho}$ to $G_{\mathbb{Q}(\sqrt{pr})} \subset G_{\mathbb{Q}}$. Since $\mathbb{Q}(\sqrt{pr})$ is linearly disjoint from N over $\mathbb{Q}$, $\tilde{\rho}_{pr}$ factors through a faithful projective representation of $\mathrm{Gal}(N(\sqrt{pr})/\mathbb{Q}(\sqrt{pr}))$ into $\mathrm{PGL}_2(\mathbb{C})$.

Because $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{pr}))$ is one of the groups appearing in case (b) of Lemma 4.2, there is a two-dimensional Galois representation

$$\rho_L : G_{\mathbb{Q}(\sqrt{pr})} \to \mathrm{GL}_2(\mathbb{C})$$

which lifts the projective representation $\tilde{\rho}_{pr}$. Let

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$$

be the representation specified in Lemma 6.3, so that ρ is a lifting of $\tilde{\rho}$. Because of hypothesis (a) of Proposition 6.6, we must be in case (b) of Lemma 6.3. The restriction ρ_{pr} of ρ to $G_{\mathbb{Q}(\sqrt{pr})}$ is also a lifting of $\tilde{\rho}_{pr}$. Thus there must be a one-dimensional character $\chi : G_{\mathbb{Q}(\sqrt{pr})} \to \mathbb{C}^*$ such that

$$\rho_L = \chi \otimes \rho_{pr}. \tag{6.8}$$

Let $\mathcal{P}$ be the unique prime over p in $\mathbb{Q}(\sqrt{pr})$. Since ρ_{pr} and ρ_L are unramified outside $\{p\}$, χ must be unramified outside $\{\mathcal{P}\}$. Because we are in case (b) of Lemma 6.3, N'/N is ramified above p, so that ρ_{pr} is ramified at all places above $\mathcal{P}$. Since ρ_L is everywhere unramified and both N'/N and $L/N(\sqrt{pr})$ are of degree 2, the character χ in (6.8) must be quadratically ramified at $\mathcal{P}$. However, Lemma 6.5 shows that no such χ exist. The contradiction shows that it is impossible for $T = \mathrm{Gal}(L/N(\sqrt{pr}))$ to be $\mathbb{Z}/2$.

It remains to consider the possibility that $T = V$ is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$ with action by $\mathrm{Gal}(N(\sqrt{pr})/\mathbb{Q}) = S_4 \times \mathbb{Z}/2$ inflated from the two-dimensional simple represention of S_4 over $\mathbb{Z}/2$. Note that $\mathbb{Q}(\sqrt{r}) \subset N(\sqrt{pr})$ since $\mathbb{Q}(\sqrt{p}) \subset N$, so $N(\sqrt{pr}) = N(\sqrt{r})$. The composition

$$\mathrm{Gal}(N(\sqrt{pr})/\mathbb{Q}(\sqrt{r})) \to \mathrm{Gal}(N(\sqrt{pr})/\mathbb{Q}) \to \mathrm{Gal}(N/\mathbb{Q}) = S_4$$

is an isomorphism, where the first map is the natural inclusion and the second one is restriction of automorphisms from $N(\sqrt{pr})$ to N. This is because an automorphism in the kernel of this map would fix both N and $\mathbb{Q}(\sqrt{r})$ elementwise, and hence would fix $N(\sqrt{pr}) = N(\sqrt{r})$. Since L is Galois over $\mathbb{Q}$, it is Galois over $\mathbb{Q}(\sqrt{r})$, and we get an exact sequence

$$1 \to \mathrm{Gal}(L/N(\sqrt{pr})) \to \mathrm{Gal}(L/\mathbb{Q}(\sqrt{r})) \to \mathrm{Gal}(N(\sqrt{pr})/\mathbb{Q}(\sqrt{r})) \to 1$$

which has the form

$$1 \to V \to \mathrm{Gal}(L/\mathbb{Q}(\sqrt{r})) \to S_4 \to 1.$$

With this identification, V still corresponds to the simple module for S_4 over $\mathbb{Z}/2$ of order 4, since a group element of order 3 in S_4 has to act non-trivially on V. Thus the possibilities for $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{r}))$ are described in Lemma 4.3. Let F_3 be a cubic subfield of N, so that $F_3(\sqrt{r})$ is a cubic extension of $\mathbb{Q}(\sqrt{r})$ inside $N(\sqrt{r})$. From Lemma 4.3, we see that there must be a degree eight abelian extension F' of $F_3(\sqrt{r})$ which lies inside L.

Since $L/\mathbb{Q}(\sqrt{pr})$ is unramified, p and r are quadratically ramified in L. Since every prime over r is already quadratically ramified in $F_3(\sqrt{r})$, we see that F' cannot ramify over any prime over r in $F_3(\sqrt{r})$. It follows that $F'/F_3(\sqrt{r})$ is unramified outside the primes over p in $F_3(\sqrt{r})$. By Proposition 6.2, p splits in F_3 as $\mathcal{Q}_1^2\mathcal{Q}_2$, where $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are degree 1 primes. Now r is not a square mod p by assumption, and the residue fields of each of $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are isomorphic to $\mathbb{Z}/p$. Hence in $F_3(\sqrt{r})$, $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are inert, and p splits as $(p) = (\mathcal{Q}_1')^2\mathcal{Q}_2'$ where $\mathcal{Q}_1'$ and $\mathcal{Q}_2'$ have degree 2. Since $\mathcal{Q}_1'$ is already quadratically ramified in $F_3(\sqrt{r})$, and the primes over p in F' can be at most quadratically ramified, we conclude that $F'/F_3(\sqrt{r})$ can be ramified only at $\mathcal{Q}_2'$, and that this extension is at most quadratically ramified over $\mathcal{Q}_2'$.

As usual, we have an exact sequence

$$1 \to \frac{k(\mathcal{Q}_2')^*}{\mathrm{Image}(O_{F_3(\sqrt{r})}^*)} \to Cl_{\mathcal{Q}_2'}(F_3(\sqrt{r})) \to Cl(F_3(\sqrt{r})) \to 1 \tag{6.9}$$

The group $\dfrac{k(\mathcal{Q}_2')^*}{k(\mathcal{Q}_2')^{*2}}$ has order 2 and we have assumed that 2 exactly divides the order of $Cl(F_3(\sqrt{r}))$. Let Cl' be the quotient of $Cl_{\mathcal{Q}_2'}(F_3(\sqrt{r}))$ by the image of $k(\mathcal{Q}_2')^{*2}$ under the homomorphism coming from (6.9). We conclude from (6.9) that the order of the Sylow 2-subgroup of Cl' is at most 4. However, the Artin map $Cl_{\mathcal{Q}_2'}(F_3(\sqrt{r})) \to \mathrm{Gal}(F'/F_3(\sqrt{r}))$ is surjective, and is trivial on the image of $k(\mathcal{Q}_2')^{*2}$ since $\mathcal{Q}_2'$ is at most quadratically ramified in F'. Thus the Artin map should factor through Cl'. This is impossible because $\mathrm{Gal}(F'/F_3(\sqrt{r}))$ is supposed to have order 8. The contradiction completes the proof of Proposition 6.6. □

Proof of Theorem 6.1.
We first produce one pair of primes (p, r) for which the hypotheses of Proposition 6.6 hold. Let $p = 14197$ and $r = 5$. Then $p \equiv 5 \bmod 8$, $r \equiv 1 \bmod 4$ and $\left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = 1$. From the tables of quartic fields computed using PARI (see [21]), the polynomial $f(x) = x^4 - 6x^2 - 3x + 1$ has four real roots, and if x_1 is one of these then $F_4 = \mathbb{Q}(x_1)$ has discriminant p. We also see from these tables that the Galois closure N of F_4 over $\mathbb{Q}$ has Galois group S_4 over $\mathbb{Q}$, the class number of F_4 is one, the ring of integers of F_4 is $O_{F_4} = \mathbb{Z}[x_1]$ and the unit group $O_{F_4}^*$ is generated by $\{\pm 1, x_1, 1 + x_1, -2 - 2x_1 + x_1^2\}$. Factoring $f(x)$ mod p gives

$$f(x) \equiv (x + 6607)^2 \cdot (x + 5272) \cdot (x + 9908) \mod p\mathbb{Z}.$$

Define $\mathcal{P}_1$, $\mathcal{P}_2$ and $\mathcal{P}_3$ to be the unique primes over p in O_{F_4} for which x_1 is congruent to -6607, -5272 and -9908, respectively. The residue field $k(\mathcal{P}_2)$ is isomorphic to $\mathbb{Z}/p$, and $3549 = (p-1)/4 = \#k(\mathcal{P}_2)^*/4$. Hence the map $\alpha \to \alpha^{3549}$ maps $k(\mathcal{P}_2)^*$ onto the group of fourth roots of unity in $k(\mathcal{P}_2)^*$ and is an isomorphism on the Sylow 2-subgroup of $k(\mathcal{P}_2)^*$. This map sends the unit $1 + x_1$ to $(1 - 5272)^{3549} \equiv 2386 \bmod p$, which is not $\pm 1 \bmod p$. Hence $1 + x_1$ is not a square in $k(\mathcal{P}_2)^*$. A cubic subfield F_3 of N is $\mathbb{Q}(y_1)$ when y_1 is one of the roots of $y^3 - 16y - 9$. The field $F_3(\sqrt{5})$ is generated over $\mathbb{Q}$ by $\sqrt{5}y_1$, which has minimal polynomial $g(y) = y^6 - 160y^4 + 6400y^2 - 10125$

over $\mathbb{Q}$. We would like to thank Jing Long for using PARI to check unconditionally that the class number of the field $F_3(\sqrt{5})$ is 2. We see from these computations that all of the hypotheses of Proposition 6.6 are satisfied when $(p, r) = (14197, 5)$. Theorem 6.1 now follows from the following result.

Proposition 6.7. *Suppose that p and r are primes satisfying the conditions of Proposition 6.6. Let N be the field described in Proposition 6.2. Fixing p, there is a set of odd primes $q \neq p$ having positive Dirichlet density for which $N(\sqrt{pq})$ is an unramified S_4-extension of $\mathbb{Q}(\sqrt{pq})$ which has odd class number. For all such q, the resulting surjection*

$$\pi : G_{\mathbb{Q}(\sqrt{pq}),\emptyset} \to \mathrm{Gal}(N(\sqrt{pq})/\mathbb{Q}(\sqrt{pq})) \cong S_4$$

shows that S_4 caps $G_{\mathbb{Q}(\sqrt{pq}),\emptyset}$ for $\ell = 2$.

Proof. Let L be the extension of N obtained by adjoining the square roots of all the units of N. Then $\mathrm{Gal}(L/N)$ is a finite elementary abelian two-group, and $L/\mathbb{Q}$ is a finite Galois extension which is unramified outside $\{2, p, \infty\}$. We aim to show that if the Frobenius conjugacy classes of r and of q in $\mathrm{Gal}(L/\mathbb{Q})$ are the same, then $N(\sqrt{pq})$ has the properties stated in the Proposition.

Note first that since $N(\sqrt{pr})$ has odd class number and is a quadratic extension of N which ramifies over the primes of N lying over r, the class number of N must also be odd. Suppose that $\mathcal{Q}_1, \ldots, \mathcal{Q}_m$ are the distinct primes over q in N. Since $\mathbb{Q}(\sqrt{p}) \subset N$ we have $N(\sqrt{pq}) = N(\sqrt{q})$. The primes of N which ramify in $N(\sqrt{pq}) = N(\sqrt{q})$ are thus exactly $\mathcal{Q}_1, \ldots, \mathcal{Q}_m$, and each of these is quadratically ramified. By genus theory, to show that $N(\sqrt{pq})$ has odd class number, it will suffice to show that the cokernel of the natural homomorphism

$$O_N^* \to \bigoplus_{i=1}^{m} \frac{k(\mathcal{Q}_i)^*}{k(\mathcal{Q}_i)^{*2}} \tag{6.10}$$

has order 2. More precisely, it will suffice to show that the image of this homomorphism is exactly the kernel of the homomorphism

$$\bigoplus_{i=1}^{m} \frac{k(\mathcal{Q}_i)^*}{k(\mathcal{Q}_i)^{*2}} \to \{\pm 1\} \tag{6.11}$$

which is induced by identifying each factor $\dfrac{k(\mathcal{Q}_i)^*}{k(\mathcal{Q}_i)^{*2}}$ with $\{\pm 1\}$ and which comes from the quadratic extension $N(\sqrt{pq})/N$.

Let $\mathcal{Q} = \mathcal{Q}_1$, and let $G_{\mathcal{Q}}$ be the decomposition group of $\mathcal{Q}$ in $G = \mathrm{Gal}(N/\mathbb{Q}) \cong S_4$. Let Ω be a set of left coset representatives for $G_{\mathcal{Q}}$ in G. Then each of the $\mathcal{Q}_i$ equals $\omega_i \mathcal{Q}$ for a unique $\omega_i \in \Omega$. Let $t = \#\Omega = 24/m$ and suppose $\alpha = \sum_{i=1}^{t} a_i \omega_i$ is an element of the group ring of G over $\mathbb{Z}/2$ which is a sum of elements of Ω. To α we can associate the homomorphism

$$l_\alpha : \bigoplus_{i=1}^{m} \frac{k(\mathcal{Q}_i)^*}{k(\mathcal{Q}_i)^{*2}} \to \{\pm 1\}$$

defined by

$$l_\alpha(\oplus_{i=1}^{m} \beta_i) = \prod_{i=1}^{m} \beta_i^{a_i}$$

where as before we identify each $\dfrac{k(\mathcal{Q}_i)^*}{k(\mathcal{Q}_i)^{*2}}$ with $\{\pm 1\}$. We have to show that the only α for which $l_\alpha(O_N^*) = 1$ are $\alpha = 0$ and $\alpha = \sum_{i=1}^{t} \omega_i$.

Suppose that α is such that $l_\alpha(O_N^*) = 1$. This means that for all units $\beta \in O_N^*$ we have

$$l_\alpha(\beta) = \prod_{i=1}^{m} \left(\frac{\beta}{\omega_i \mathcal{Q}} \right)^{a_i} = 1$$

where $\left(\frac{*}{\omega_i\mathcal{Q}}\right)$ is the quadratic residue symbol associated to the prime ideal $\omega_i\mathcal{Q}$. By definition,

$$\left(\frac{\beta}{\omega_i\mathcal{Q}}\right) = \left(\frac{\omega_i^{-1}(\beta)}{\mathcal{Q}}\right).$$

Thus $l_\alpha(O_N^*) = 1$ if and only if

$$\left(\frac{z_\alpha(\beta)}{\mathcal{Q}}\right) = 1$$

for all units $\beta \in O_N^*$, where $z_\alpha : O_N^* \to O_N^*$ is the homomorphism defined by

$$z_\alpha(\beta) = \prod_{i=1}^{m} \omega_i^{-1}(\beta)^{a_i}.$$

This is equivalent to the statement that every unit in $z_\alpha(O_N^*)$ is a square in $k(\mathcal{Q})$. It follows that $l_\alpha(O_N^*) = 1$ if and only if $\mathcal{Q}$ splits in the extension $N(\sqrt{z_\alpha(O_N^*)})$ of N obtained by adjoining the square roots of all units in the subgroup $z_\alpha(O_N^*)$ of O_N^*.

We can thus say that $N(\sqrt{pq})$ has odd class number if and only if the following is true. Suppose α is a formal combination $\alpha = \sum_{i=1}^t a_i\omega_i$ in which the a_i are in $\mathbb{Z}/2$, and that $a_i \neq a_j$ for some i and j. Then $\mathcal{Q}$ does not split completely in the extension $N(\sqrt{z_\alpha(O_N^*)})$ of N.

We now suppose that q and r are primes different from 2 and p which have the same Frobenius conjugacy class in $\mathrm{Gal}(L/\mathbb{Q})$ when L is the extension of N obtained by adjoining the square roots of all the units of N. We can then choose primes $\hat{\mathcal{R}}$ over r and $\hat{\mathcal{Q}}$ over q in L which have the same Frobenius automorphism in $\mathrm{Gal}(L/\mathbb{Q})$; call this Frobenius σ. Let $\mathcal{R}$ and $\mathcal{Q}$ be the primes of N determined by $\hat{\mathcal{R}}$ and $\hat{\mathcal{Q}}$. The image of σ in $\mathrm{Gal}(N/\mathbb{Q})$ is then the Frobenius automorphism for both $\mathcal{R}$ and $\mathcal{Q}$, so these primes have the same decomposition group $\mathfrak{D}(G,\mathcal{Q}) = \mathfrak{D}(G,\mathcal{R})$ in $G = \mathrm{Gal}(N/\mathbb{Q})$. We fix a set of coset representatives Ω for $\mathfrak{D}(G,\mathcal{Q}) = \mathfrak{D}(G,\mathcal{R})$ as above. Because we know that $N(\sqrt{pr})$ has odd class number, we know that for every $\alpha = \sum_{i=1}^t a_i\omega_i$ as above such that $a_i \neq a_j$ for some i and j, the prime $\mathcal{R}$ does not split in the extension $N(\sqrt{z_\alpha(O_N^*)})$. Suppose

$$\mathrm{Frob}_{N/\mathbb{Q}}(\mathcal{Q}) = \mathrm{Frob}_{N/\mathbb{Q}}(\mathcal{R}) = \overline{\sigma}$$

has order s. Then $\mathrm{Frob}_{L/N}(\hat{\mathcal{Q}}) = \sigma^s = \mathrm{Frob}_{L/N}(\hat{\mathcal{R}})$. The statement that $\mathcal{R}$ does not split in the extension $N(\sqrt{z_\alpha(O_N^*)})$ is the same as saying that $\mathrm{Frob}_{L/N}(\hat{\mathcal{R}}) = \sigma^s$ does not lie in the subgroup $\mathrm{Gal}(L/N(\sqrt{z_\alpha(O_N^*)}))$ of $\mathrm{Gal}(L/N)$. Since the truth or falsity of this last statement for a given α does not change if we replace $\mathcal{R}$ by $\mathcal{Q}$, we conclude that $N(\sqrt{pq})$ has to have odd class number because $N(\sqrt{pr})$ does. The last statement of Proposition 6.7 follows from Remark 3.8. □

7. Singularities of deformation rings

In this section we consider the following Question which was mentioned in the introduction:

Question 7.1. *Suppose k is a field of characteristic $\ell > 0$, G is a finite group and that V is a kG-module of finite dimension over k which belongs to a block B of kG having a defect group D which has nilpotency r. Suppose further that the stable endomorphism ring $\underline{\mathrm{End}}_{kG}(V)$ of V is one-dimensional over k, so that $R(G,V)$ is well defined. Is it the case that $\dim(R(G,V)) - \mathrm{depth}(R(G,V)) \leq r-1$?*

Theorem 7.2. *Suppose k is algebraically closed. Question 7.1 has an affirmative answer in the following cases:*

i. $\dim_k(V) = 1$.
ii. *D is cyclic or a Klein four group.*
iii. *V is the two-dimensional irreducible representation of S_4 and $\ell = 2$.*
iv. *D is dihedral of order at least 8, $\ell = 2$ and B is Morita equivalent to the principal 2-block of a finite simple group.*

In cases (i) and (ii), $r = 1$ and $R(G,V)$ is a complete intersection. In cases (iii) and (iv), $r = 2$.

Proof. Suppose first that $\dim_k(V) = 1$ as in part (i) of the Theorem, so that $R(G,V) = WG^{ab,\ell}$ by [20, §1.4]. Since $G^{ab,\ell}$ is a finite abelian ℓ-group, it is a direct sum of cyclic ℓ-groups $\mathbb{Z}/\ell^n$ for various integers $n \geq 0$. There is an isomorphism $W[[t]]/((t+1)^{\ell^n}-1) \to W(\mathbb{Z}/\ell^n)$ sending t to $\sigma - 1$ if σ generates $\mathbb{Z}/\ell^n$. Therefore, $WG^{ab,\ell}$ is isomorphic to the tensor product over W of W-algebras of the form $W[[t]]/((t+1)^{\ell^n}-1)$, and is thus a complete intersection.

Suppose now that D is cyclic of order ℓ^d. Then the number e of non-isomorphic simple B-modules is a divisor of $\ell - 1$. Let E be the unique cyclic subgroup of $\mathrm{Aut}(D)$ of order e. Then E acts on the group ring WD. Let $s = \sum_{x \in D} x \in WD$. It follows from [3] that the universal deformation ring $R(G,V)$ is isomorphic to one of the following W-algebras: W, W/ℓ^d, WD or $(WD)^E/Ws$, where $(WD)^E$ is the subring of E-invariants in WD. The rings W, W/ℓ^d and $WD \cong W[[t]]/((t+1)^{\ell^d}-1)$ are complete intersections. Suppose now that $R = R(G,V) = (WD)^E/Ws$ as in the remaining case. By [3, §4], $R/\ell R$ is isomorphic to $k[t]/(t^r)$ as a W-algebra when $r = \mathrm{rank}_W R$. Hence there is a surjection $\pi : W[[t]] \to R$. Since R is free of rank r over W, there is a monic polynomial $g(t) \in W[t]$ of degree r contained in $\mathrm{Ker}(\pi)$. Hence there is a surjection $W[[t]]/(g(t)) \to R/\ell R = k[t]/(t^r)$ sending t to t. This forces all of the non-leading coefficients of $g(t)$ to be divisible by ℓ, so $g(t)$ is a distinguished polynomial in $W[[t]]$, and $W[[t]]/(g(t)) = W[t]/(g(t))$. Now we have a surjection $W[t]/(g(t)) \to R$, so since these rings are free W-modules of the same rank r, this surjection must be an isomorphism. Because R has dimension 1, this shows that R is a complete intersection.

If D is a Klein four group, so that $\ell = 2$, it follows from [1, §3] that $R(G,V)$ is isomorphic to either W, k or WD. The rings W and k are complete intersections. Using the same argument as in the $\dim_k(V) = 1$ case, it follows that WD is also a complete intersection.

We now suppose that V is the two-dimensional irreducible representation of $G = S_4$ in characteristic $\ell = 2$. Then $R(G,V) = W[[t]]/(t^2, 2t)$ by Theorem 2.3. Since the defect groups of the block of V are dihedral groups of order 8, their nilpotency is $r = 2$. Thus case (iii) follows from the fact that

$$\dim(R(G,V)) - \mathrm{depth}(R(G,V)) = 1 - 0 = r - 1.$$

Finally suppose V is as in case (iv) of Theorem 7.2. It follows from [2] that $R(G,V)$ is either W, $W/2^m$ for some $m \geq 1$ or $W[[t]]/(t \cdot f(t), 2 \cdot f(t))$ for some distinguished polynomial $f(t) \in W[[t]]$. The rings W and $W/2^m$ are complete intersections. Suppose now that $R(G,V) \cong W[[t]]/I$ where $I = (t \cdot f(t), 2 \cdot f(t))$ as in the remaining case. Since $W[[t]]$ has dimension 2, and $(t \cdot f(t)) \subset I \subset (f(t))$, we see that $\dim(R(G,V)) = 1$. Because the defect groups of the block of V have nilpotency 2, we conclude that

$$\dim(R(G,V)) - \mathrm{depth}(R(G,V)) \leq 1 = r - 1.$$

This completes the proof of Theorem 7.2. □

References

[1] F. M. Bleher, Universal deformation rings and Klein four defect groups. Trans. Amer. Math. Soc. 354 (2002), 3893–3906.

[2] F. M. Bleher, Universal deformation rings and dihedral defect groups. Preprint, 2006.

[3] F. M. Bleher and T. Chinburg, Universal deformation rings and cyclic blocks. Math. Ann. 318 (2000), 805–836.

[4] F. M. Bleher and T. Chinburg, Applications of versal deformations to Galois theory. Comment. Math. Helv. 78 (2003), 45–64.

[5] F. M. Bleher and T. Chinburg, Universal deformation rings need not be complete intersections. C. R. Math. Acad. Sci. Paris 342 (2006), 229–232.

[6] G. Böckle, On the density of modular points in universal deformation spaces. Amer. J. Math. 123 (2001), 985–1007.

[7] G. Böckle, C. Khare. Mod l representations of arithmetic fundamental groups. II. A conjecture of A. J. de Jong. Compos. Math. 142 (2006), 271–294.

[8] N. Boston, Galois p-groups unramified at p - a survey, to appear in the JAMI proceedings "Knots and Primes".

[9] T. Chinburg, Can deformation rings of group representations not be local complete intersections? In: Problems from the Workshop on Automorphisms of Curves. Edited by Gunther Cornelissen and Frans Oort, with contributions by I. Bouw, T. Chinburg, Cornelissen, C. Gasbarri, D. Glass, C. Lehr, M. Matignon, Oort, R. Pries and S. Wewers. Rend. Sem. Mat. Univ. Padova 113 (2005), 129–177.

[10] A. J. de Jong, A conjecture on arithmetic fundamental groups. Israel J. Math. 121 (2001), 61–84.

[11] B. de Smit and H. W. Lenstra, 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.
[12] M. Emerton and F. Calegari, On the ramification of Hecke algebras at Eisenstein primes. Invent. Math. 160 (2005), 97–144.
[13] M. Emerton, R. Pollack and T. Weston, Variation of Iwasawa invariants in Hida families. Invent. Math. 163 (2006), 523–580.
[14] A. Fröhlich, Artin root numbers, conductors, and representations for generalized quaternion groups. Proc. London Math. Soc. (3) 28 (1974), 402–438.
[15] D. Gaitsgory, On de Jong's conjecture. ArXiv math.AG/0402184.
[16] A. Grothendieck, Éléments de géométrie algébrique, Chapitre IV, Quatriéme Partie. Publ. Math. IHES 32 (1967), 5–361.
[17] B. Huppert, Endliche Gruppen I, Grundlehren der math. Wissenschaften, Vol. 134, Springer-Verlag, Berlin-Heidelberg-New York, 1983.
[18] M. Kisin, Overconvergent modular forms and the Fontaine-Mazur conjecture. Invent. Math. 153 (2003), 373–454.
[19] M. Kisin, Moduli of finite flat group schemes and modularity. Preprint, 2006.
[20] B. Mazur, Deforming Galois representations. In: Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), Springer-Verlag, Berlin-Heidelberg-New York, 1989, pp. 385–437.
[21] PARI2, PARI/GP, version 2.1.5, Bordeaux, 2004, `http://pari.math.u-bordeaux.fr/` and `ftp://megrez.math.u-bordeaux.fr/pub/numberfields/`.
[22] J. P. Serre, Modular forms of weight one and Galois representations. In: Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 193–268.
[23] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras. Ann. of Math. 141 (1995), 553–572.
[24] L. C. Washington, Introduction to Cyclotomic Fields. Springer-Verlag, New York, 1982.
[25] A. Wiles, Modular elliptic curves and Fermat's last theorem. Ann. of Math. 141 (1995), 443–551.

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

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