

Galois representations with open image

Ralph Greenberg[†]

1 Introduction.

Suppose that p is a prime and that $n \geq 1$. Let $G_{\mathbf{Q}} = \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ be the absolute Galois group of \mathbf{Q} . Our objective in this paper is to construct continuous representations

$$\rho : G_{\mathbf{Q}} \longrightarrow GL_n(\mathbf{Z}_p)$$

whose image is open. Continuous n -dimensional representations ρ arise naturally in algebraic geometry for every value of n , but it seems difficult to find such examples where the image is open when $n \geq 3$. The construction described in this paper is not at all geometric in nature. It depends on the structure of certain Galois groups and of certain subgroups of $GL_n(\mathbf{Z}_p)$. We assume always that p is an odd prime. One typical result is the following.

Proposition 1.1. *Suppose that p is a regular prime and that $p \geq 4\lfloor \frac{n}{2} \rfloor + 1$. Let $K = \mathbf{Q}(\mu_p)$ and let M denote the maximal pro- p extension of K which is unramified outside of p . Then there exist continuous representations $\rho : \text{Gal}(M/\mathbf{Q}) \rightarrow GL_n(\mathbf{Z}_p)$ with an open image.*

The assumption that p is regular turns out to imply that $\text{Gal}(M/K)$ is a free pro- p group on $\frac{p+1}{2}$ generators. On the other hand, it turns out that a Sylow pro- p subgroup S_0 of $SL_n(\mathbf{Z}_p)$ requires only n generators topologically. This allows one to define a surjective homomorphism σ_0 from $\text{Gal}(M/K)$ to S_0 if $p \geq 2n - 1$. There are many choices. However, one must make the definition carefully enough so that σ_0 can be extended to $\text{Gal}(M/\mathbf{Q})$, giving a homomorphism $\rho_0 : \text{Gal}(M/\mathbf{Q}) \rightarrow GL_n(\mathbf{Z}_p)$. If n is even, one needs the slightly stronger inequality $p \geq 2n + 1$ to make that possible. The image of ρ_0 will then contain S_0 as a subgroup whose index divides $p - 1$. Tensoring ρ_0 by the cyclotomic character gives a representation ρ with open image. It turns out that the construction gives uncountably many such ρ 's with distinct kernels.

[†]Research supported in part by National Science Foundation grant DMS-0200785.

One can prove a similar result for more pairs (n, p) by making different choices for the field K . One useful choice is to take K to be a compositum of quadratic fields. We can then construct representations for any $n \geq 4$ and any odd prime p if we make a reasonable conjecture concerning class numbers and p -adic regulators for such fields. The precise statement is conjecture 4.2.1 and involves the notion of a p -rational number field which is discussed in section 3.

The proof of proposition 1.1 in section 6 constructs representations ρ having the following property: the residual representation $\bar{\rho}$ is reducible. More precisely, the image of $\bar{\rho}$ consists of upper triangular matrices. In section 7, we will discuss some possible examples where $\bar{\rho}$ is irreducible. The approach is based on the discussion in [Bos] of automorphism groups of pro- p groups and is closely related to deformation theory for the special case where the image of $\bar{\rho}$ has order prime to p . In fact, our approach is essentially just a straightforward application of the group-theoretic observations found in the first few pages of Boston's paper.

One specific type of example is the following. Suppose that K is a totally complex Galois extension of \mathbf{Q} such that $\Omega = \text{Gal}(K/\mathbf{Q})$ is isomorphic to the symmetric group S_{n+1} . If $p > n + 1$, then Ω has an absolutely irreducible representation ω over \mathbf{Q}_p of degree n . It is a direct summand in the obvious permutation representation of Ω of degree $n + 1$. One can realize ω over \mathbf{Z}_p and $\bar{\omega}$, the reduction of ω modulo p , is still absolutely irreducible. Under the assumption that K is p -rational, we will show that there exists an n -dimensional representation ρ of $\text{Gal}(M/\mathbf{Q})$ over \mathbf{Z}_p with open image such that $\bar{\rho} \cong \bar{\omega}$. Here M is defined just as in proposition 1.1. Although it would be difficult to verify the assumption that K is p -rational when $n \geq 3$, it is reasonable to believe that it is satisfied for all but an extremely sparse, infinite set of primes. Many extensions K of \mathbf{Q} exist with the specified Galois group, and varying that choice certainly increases the chance that one of them will be p -rational for any given prime p .

Galois representations with open image have already been constructed by S. Hamblen for $n = 3$ and $p \equiv 8 \pmod{21}$. Such examples come from his main theorems in [Ham] showing that n -dimensional representations $\bar{\rho}$ of $G_{\mathbf{Q}}$ over \mathbf{F}_p can be lifted to representations ρ over \mathbf{Z}_p under certain hypotheses. Then, for certain choices of $\bar{\rho}$, Hamblen shows that there exist liftings ρ with open image. The representation ρ is unramified outside a finite set of primes. His specific examples are at the end [Ham]. The field K is the splitting field of a certain polynomial of degree 7 and $\Omega = \text{Gal}(K/\mathbf{Q})$ is the simple group of order 168. The representation $\bar{\rho}$ is absolutely irreducible, one of the two such representations of Ω of degree 3. His construction of ρ 's provides examples with certain specified local properties. In addition, in one of his examples, K is totally real and he then obtains representations ρ such that $\overline{\mathbf{Q}}^{\ker(\rho)}$ is also totally real.

Another interesting source of examples has been found by M. Upton [Upt]. Her examples

are 3-dimensional Galois representations of G_F , where F is any number field containing $\mathbf{Q}(\mu_3)$. They arise in a geometric way, namely from the action of G_F on the p -adic Tate module $T_p(J)$, where J is the Jacobian variety of a Picard curve C defined over F . The genus of C is 3 and $\text{End}_F(J)$ contains $\mathbf{Z}[\mu_3]$. Thus, $T_p(J)$ can be viewed as a free module of rank 3 over the ring $R = \mathbf{Z}[\mu_3] \otimes_{\mathbf{Z}} \mathbf{Z}_p$. There is an R -linear action of G_F on $T_p(J)$. Choosing a basis, one obtains a homomorphism $r : G_F \rightarrow GL_3(R)$. If $p \equiv 1 \pmod{3}$, then $R \cong \mathbf{Z}_p \times \mathbf{Z}_p$ and one obtains a representation $\rho : G_F \rightarrow GL_3(\mathbf{Z}_p)$ by projection to either factor. Upton shows that if $\text{End}_F(J) = \mathbf{Z}[\mu_3]$, then ρ is surjective for all but finitely many such p 's. It is likely that the image of ρ is open for all such primes p .

The topic of this paper arose in connection with a project concerning Iwasawa theory for elliptic curves. It was of interest to construct examples of Galois extensions of \mathbf{Q} whose Galois group is isomorphic to a certain open subgroup H_∞ of $PGL_2(\mathbf{Z}_p)$. Such extensions play a role in the illustrations in chapters 8 and 13 of [Gr1]. The proof of proposition 1.1 for the special case $n = 2$ provides many such examples when p is a regular prime. The representation theory of the finite quotient groups of H_∞ is described rather precisely in proposition 7.4.4 in the above paper. Realizing H_∞ as a Galois group over \mathbf{Q} provides infinite families of irreducible Artin representations over \mathbf{Q} whose degrees and modular properties are known. Many of those Artin representations are self-dual, and that makes them especially interesting to study.

I am grateful to Robert Pollack for asking me if the construction that I found for $n = 2$ could be extended to similarly defined subgroups of $PGL_n(\mathbf{Z}_p)$, which led to proposition 1.1. I also want to thank Sourav Sen Gupta and Robert Bradshaw who carried out searches for compositums of quadratic fields which are 3-rational. Bradshaw also showed me how to use Sage for carrying out a search concerning the p -rationality of $\mathbf{Q}(\mu_5)$. Finally, I want to acknowledge support for this research from the National Science Foundation.

2 Pro- p groups with operators.

Assume that Π is a pro- p group. We will always assume that Π is topologically finitely generated. This means that we can find a finite subset $\Sigma = \{\pi_1, \dots, \pi_t\}$ of Π such that the subgroup $\langle \pi_1, \dots, \pi_t \rangle$ generated by Σ is dense in Π . Let $\Phi(\Pi)$ denote the Frattini subgroup of Π , which is defined to be the intersection of all closed subgroups of Π of index p . We will refer to the quotient $\tilde{\Pi} = \Pi/\Phi(\Pi)$ as the Frattini quotient of Π . Note that $\tilde{\Pi}$ is an abelian group of exponent p . We regard $\tilde{\Pi}$ as a vector space over \mathbf{F}_p . If $\pi \in \Pi$, then its image in $\tilde{\Pi}$ will be denoted by $\tilde{\pi}$. It is clear that if $\{\pi_1, \dots, \pi_t\}$ is a topological generating set for Π , then

$\{\tilde{\pi}_1, \dots, \tilde{\pi}_t\}$ generates $\tilde{\Pi}$ as an \mathbf{F}_p -vector space. The Burnside Basis Theorem is the converse:

BBT: *If $\{\tilde{\pi}_1, \dots, \tilde{\pi}_t\}$ generates $\tilde{\Pi}$, then $\{\pi_1, \dots, \pi_t\}$ generates Π topologically.*

In particular, if $d = \dim_{\mathbf{F}_p}(\tilde{\Pi})$, then Π has a topological generating set with d elements, but not fewer. Note that $d = \dim_{\mathbf{F}_p}(H^1(\Pi, \mathbf{F}_p))$, where Π acts trivially on \mathbf{F}_p .

Suppose that Π_1 and Π_2 are pro- p groups, both topologically finitely generated. Suppose that $\sigma : \Pi_1 \rightarrow \Pi_2$ is a continuous group homomorphism. Then σ induces a homomorphism from $\tilde{\Pi}_1$ to $\tilde{\Pi}_2$ which we denote by $\tilde{\sigma}$. It follows easily from **BBT** that σ is surjective if and only if $\tilde{\sigma}$ is surjective.

We will need the profinite version of the Schur-Zassenhaus theorem in this paper. It will be used several times in the following form. The group G will sometimes be a Galois group, sometimes a subgroup of $GL_n(\mathbf{Z}_p)$, and sometimes a subgroup of $\text{Aut}(\Pi)$, the group of continuous automorphisms of a pro- p group Π .

SZT: *Suppose that G is a profinite group, that N is a normal pro- p subgroup of G , and that G/N is a finite group of order prime to p . Then G contains a subgroup H such that $G = HN$ and $H \cap N = \{id_G\}$. Furthermore, all such subgroups of G are conjugate.*

The usual form of the Schur-Zassenhaus theorem concerns finite groups and can be found in [Gor], theorem 2.1. Extending it from finite to profinite groups is not difficult. Note that if G, N , and H are as in **SZT**, then we obviously have $H \cong G/N$. The theorem means that G is isomorphic to a semidirect product $N \rtimes H$, where H acts on N by conjugation. Furthermore, it follows that if H and H' are two such subgroups, then we have $H' = nHn^{-1}$ for some $n \in N$.

2.1. The Ω -type. Now suppose that Ω is a finite group of order prime to p . Let $\text{Aut}(\Pi)$ denote the group of continuous automorphisms of Π . Suppose that we are given a homomorphism $\Omega \rightarrow \text{Aut}(\Pi)$. We will then refer to Π as an Ω -group. We can view $\tilde{\Pi}$ as a finite-dimensional \mathbf{F}_p -representation space for Ω . It must be completely reducible because $p \nmid |\Omega|$. We will refer to the isomorphism class of $\tilde{\Pi}$ as the “ Ω -type” of Π . Let $\text{Irr}_{\mathbf{F}_p}(\Omega)$ be the set of isomorphism classes of \mathbf{F}_p -irreducible representations of Ω . For each χ in $\text{Irr}_{\mathbf{F}_p}(\Omega)$, let $m_\chi(\tilde{\Pi})$ denote the multiplicity of χ as a constituent in $\tilde{\Pi}$. The Ω -type of Π is determined if one knows those multiplicities for all $\chi \in \text{Irr}_{\mathbf{F}_p}(\Omega)$. Note that if Π is an Ω -group, then so is its maximal abelian quotient Π^{ab} . The Ω -types of Π and of Π^{ab} are obviously the same.

An important hypothesis in most of our results will be that Ω satisfies the following property:

Assumption A: Ω is an abelian group and every element of Ω has order dividing $p - 1$.

If this assumption is satisfied, then $\text{Irr}_{\mathbf{F}_p}(\Omega)$ can be identified with $\widehat{\Omega} = \text{Hom}(\Omega, \mathbf{F}_p^\times)$. There is a canonical homomorphism $\mathbf{F}_p^\times \rightarrow \mathbf{Z}_p^\times$ since every coset in $(\mathbf{Z}_p/p\mathbf{Z}_p)^\times$ contains a unique $(p - 1)$ -st root of unity. If $\chi \in \widehat{\Omega}$, then composing with that canonical homomorphism gives a character of Ω with values in \mathbf{Z}_p^\times . We will simply use the same letter χ for that lifting. If $\pi \in \Pi$ and $a \in \mathbf{Z}_p$, then one can define π^a . It is an element in the closure of the subgroup $\langle \pi \rangle$ generated by π , which we denote by $\overline{\langle \pi \rangle}$. Thus, it makes sense to write $\pi^{\chi(\alpha)}$ if $\pi \in \Pi$, $\alpha \in \Omega$, and $\chi \in \widehat{\Omega}$.

Assume that Π is a pro- p Ω -group and that Ω satisfies assumption **A**. We will describe a useful refinement of the Burnside Basis Theorem in this case. For $\alpha \in \Omega$ and $\pi \in \Pi$, we write $\alpha(\pi)$ for the image of π under the automorphism of Π corresponding to α . Let $\chi \in \widehat{\Omega}$. A nontrivial element $\pi \in \Pi$ will be called a “ χ -element” if $\alpha(\pi) = \pi^{\chi(\alpha)}$ for all $\alpha \in \Omega$. We will also refer to such an element $\pi \in \Pi$ as an Ω -element if we don’t specify the character χ . This simply means that $\overline{\langle \pi \rangle}$ is invariant under the action of Ω . One can find an \mathbf{F}_p -basis for $\widetilde{\Pi}$ consisting of Ω -elements. The following result together with **BBT** implies that one can lift such a basis to a set of topological generators for Π consisting of Ω -elements.

Proposition 2.1.1. *Suppose that Ω satisfies assumption **A**. Suppose that χ is a character of Ω and that z is a χ -element in $\widetilde{\Pi}$. Then there exists a χ -element x in Π such that $\tilde{x} = z$.*

This result can be found in [Bos]. It is a special case of proposition 2.3 in that paper, as is noted on page 184. We also had found it prior to learning that it was already in [Bos] since we needed it for proving proposition 1.1. It plays a central role in this paper and so we will give our proof. It is somewhat different than the argument found in [Bos], although essentially as simple.

Proof. First of all, assume that Π is abelian. Then $\Phi(\Pi) = \Pi^p$. We can regard Π and $\widetilde{\Pi} = \Pi/\Pi^p$ as $\mathbf{Z}_p[\Omega]$ -modules. We will use an exponential notation for the action of $\mathbf{Z}[\Omega]$ on Π , writing x^θ for $x \in \Pi$ and $\theta \in \mathbf{Z}_p[\Omega]$. We use the same notation for $\widetilde{\Pi}$. Let $e_\chi \in \mathbf{Z}_p[\Omega]$ denote the idempotent for χ . Then Π^{e_χ} is a direct summand of Π as a $\mathbf{Z}_p[\Omega]$ -module. We refer to Π^{e_χ} as the χ -component of Π . The χ -elements of Π are the non-trivial elements in Π^{e_χ} . The natural map $\Pi \rightarrow \widetilde{\Pi}$ induces a homomorphism $\Pi^{e_\chi} \rightarrow \widetilde{\Pi}^{e_\chi}$ which is clearly surjective. Thus, the stated result is true if Π is abelian. Furthermore, if Ψ is a subgroup of Π^p and $\Pi' = \Pi/\Psi$, then we have surjective homomorphisms $\Pi \rightarrow \Pi' \rightarrow \widetilde{\Pi}$. The corresponding homomorphisms on the χ -components are also surjective. Thus, for any χ -element x' of Π' which maps to z , there exists a χ -element x of Π which maps to x' , and hence to z .

Now assume that Π is a finite p -group, but not necessarily abelian. We prove by induction on $|\Pi|$ that there exists a χ -element $x \in \Pi$ such that $\tilde{x} = z$. We may suppose that $|\Phi(\Pi)| > 1$. Let \mathcal{Z} denote the center of Π and let $\Psi = \mathcal{Z} \cap \Phi(\Pi)$. Then Ψ is a normal, Ω -invariant subgroup of Π , $\Psi \subseteq \Phi(\Pi)$, and $|\Psi| > 1$. Let $\Pi' = \Pi/\Psi$. Then we can identify $\tilde{\Pi}'$ with $\tilde{\Pi}$. Assume (inductively) that we can find a χ -element x' in Π' whose image in $\tilde{\Pi}$ is z . Then $x' = y\Psi$, where $y \in \Pi$ and $\alpha(y) \equiv y^{\chi(\alpha)} \pmod{\Psi}$ for all $\alpha \in \Omega$. The image of y in $\tilde{\Pi}$ is z . The subgroup $\langle \Psi, y \rangle$ generated by Ψ and y will be Ω -invariant and abelian. As already shown, one can find a χ -element $x \in \langle \Psi, y \rangle$ such that $x \equiv y \pmod{\Psi}$, establishing the lemma if Π is finite.

We use a similar argument if Π is infinite. We can find a descending sequence of open, normal, Ω -invariant subgroups Ψ_j of Π , all contained in $\Phi(\Pi)$, such that $\bigcap_j \Psi_j = \{id_\Pi\}$ and Ψ_j/Ψ_{j+1} is contained in the center of Π/Ψ_{j+1} . We obtain $x \in \Pi$ with the desired properties as a compatible sequence of suitable elements $x_j \in \Pi/\Psi_j$. \blacksquare

Apart from Boston's paper mentioned above, the existence of a generating set consisting of Ω -elements has been pointed out elsewhere in the special case where Ω has order 2. For example, Herfort and Ribes [HeRi] show that if Π is a pro- p -group with an involution, and p is an odd prime, then Π has a set of topological generators which are either fixed or inverted by the given involution.

Assumption **A** will prevail throughout most of this paper. However, we sometimes will want to make the following weaker assumption, especially in section 7.

Assumption B. *The order of Ω is not divisible by p .*

Roughly speaking, the role of this assumption is partly that it makes the relationship between representation theory for Ω in characteristic 0 and in characteristic p quite simple. Also, it allows us to apply the **SZT** in several situations, e.g., the proof of proposition 2.3.1 below.

2.2. Free pro- p Ω -groups. Returning to the case where Ω is any finite group of order prime to p , suppose that Γ is a free pro- p group on d generators and that one is given a homomorphism $\psi : \Omega \rightarrow \text{Aut}_{\mathbf{F}_p}(\tilde{\Gamma})$. Of course, that homomorphism is just a d -dimensional representation of Ω over \mathbf{F}_p . We want to now show that ψ can be lifted to a homomorphism $\varphi : \Omega \rightarrow \text{Aut}(\Gamma)$. As a consequence, one can find a free Ω -group Γ with any specified Ω -type.

First of all, observe that any automorphism $\tilde{\alpha}$ of $\tilde{\Gamma}$ can be lifted to a continuous automorphism α of Γ . That is, the natural map

$$(1) \quad \text{Aut}(\Gamma) \longrightarrow \text{Aut}(\tilde{\Gamma})$$

is surjective. To see this, suppose that Γ is the free pro- p group on the set $\Sigma = \{\gamma_1, \dots, \gamma_t\}$. The universal mapping property for (Γ, Σ) implies that we can at least define a continuous homomorphism $\alpha : \Gamma \rightarrow \Gamma$ lifting $\tilde{\alpha}$. The surjectivity of α follows from **BBT**. The inflation-restriction sequence together with the fact that $H^2(\Gamma, \mathbf{F}_p) = 0$ implies easily that $H^1(\ker(\alpha), \mathbf{F}_p) = 0$. Since $\ker(\alpha)$ is a pro- p group, it follows that $\ker(\alpha)$ is trivial and hence that α is injective. The continuity of α^{-1} also follows easily.

Let N denote the kernel of the map (1). It is known that N is a pro- p group. In fact, this is true if Γ is any topologically finitely-generated pro- p group. (See proposition 5.5 in [DSMS].) Let $G \subset \text{Aut}(\Gamma)$ be the inverse image of $\psi(\Omega)$ under the map (1). Thus, G contains N and the corresponding quotient group G/N is isomorphic to $\psi(\Omega)$. Since $\psi(\Omega)$ has order prime to p , **SZT** tells us that G is a semi-direct product. That is, G contains a subgroup H such that $G = HN$ and $H \cap N = \{id_G\}$. Thus, the obvious map $H \rightarrow G/N$ is an isomorphism and therefore we have a uniquely determined surjective map $\varphi : \Omega \rightarrow H$ which induces the map $\psi : \Omega \rightarrow G/N \rightarrow \text{Aut}(\tilde{\Gamma})$, as we wanted. Since $H \subset \text{Aut}(\Gamma)$, the map φ makes Γ into an Ω -group.

Remark 2.2.1. A theorem in modular representation theory asserts that if Ω has order prime to p , then any homomorphism $\bar{\omega} : \Omega \rightarrow GL_d(\mathbf{F}_p)$ can always be lifted to a homomorphism $\omega : \Omega \rightarrow GL_d(\mathbf{Z}_p)$. In fact, the same argument as above shows this. The map $GL_d(\mathbf{Z}_p) \rightarrow GL_d(\mathbf{F}_p)$ is easily seen to be surjective. That is all one needs in the above argument. Alternatively, in the above notation, one can choose an \mathbf{F}_p -basis for $\tilde{\Gamma}$ and identify $\bar{\omega}$ with ψ . One can lift the chosen basis for $\tilde{\Gamma}$ to a set of topological generators Σ for Γ . The homomorphism φ induces a homomorphism $\varphi^{ab} : \Omega \rightarrow \text{Aut}(\Gamma^{ab})$. The set Σ maps to a \mathbf{Z}_p -module basis for Γ^{ab} and one can then identify Γ^{ab} with \mathbf{Z}_p^d . Then φ^{ab} defines a homomorphism ω which lifts $\bar{\omega}$.

If Ω has order prime to p and L is a free \mathbf{Z}_p -module of finite rank on which Ω acts, then L is a $\mathbf{Z}_p[\Omega]$ -module. It is a projective module and its isomorphism class determines and is determined by the isomorphism class of L/pL as an $\mathbf{F}_p[\Omega]$ -module. Furthermore, the isomorphism class of the $\mathbf{Q}_p[\Omega]$ -module $L \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ determines and is determined by the isomorphism class of L as a $\mathbf{Z}_p[\Omega]$ -module. One can find these useful results in [Ser], specifically in proposition 43 and in corollary 2 to theorem 34.

One consequence that we will need is the following. Suppose that Γ is a free pro- p Ω -group. Let $V = \Gamma^{ab} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. One can regard Γ^{ab} as an Ω -invariant \mathbf{Z}_p -lattice in V . Then the Ω -type of Γ determines and is determined by the isomorphism class of the \mathbf{Q}_p -representation space $V = \Gamma^{ab} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ for Ω . \diamond

The simplest examples of free pro- p Ω -groups occur when $d = 1$ and Ω is an abelian group of exponent dividing $p - 1$. Let $\chi \in \hat{\Omega}$. Regarding χ as having values in \mathbf{Z}_p^\times , we let

Γ_χ denote a group isomorphic to \mathbf{Z}_p on which Ω acts by χ . We can obviously take direct products of such groups, obtaining Ω -groups which are free, abelian pro- p groups and which have any specified Ω -type. One can also take a free product of finitely many such groups, which gives an explicit way of obtaining a free pro- p Ω -group with any specified Ω -type in the special case where Ω satisfies assumption **A**.

2.3. A universal mapping property. We only assume that Ω satisfies assumption **B**. Suppose that Π is a finitely-generated pro- p group which is also an Ω -group. The following result gives the existence of surjective Ω -homomorphisms from a free pro- p Ω -group Γ to Π if the Ω -type of Π is “bounded above” by the Ω -type of Γ .

Proposition 2.3.1. *Suppose that Γ is a free pro- p Ω -group on a finite number of generators, that Π is a pro- p Ω -group, and that there exists a surjective Ω -homomorphism*

$$\tau : \tilde{\Gamma} \rightarrow \tilde{\Pi} \quad .$$

Then there exists a surjective Ω -homomorphism $\sigma : \Gamma \rightarrow \Pi$ such that $\tilde{\sigma} = \tau$.

Note that such a τ exists if and only if $m_\chi(\tilde{\Pi}) \leq m_\chi(\tilde{\Gamma})$ for all $\chi \in \text{Irr}_{\mathbf{F}_p}(\Omega)$.

Proof. The structure of Γ as an Ω -group is given by a homomorphism $\varphi : \Omega \rightarrow \text{Aut}(\Gamma)$. Let H denote the image of φ . Let $\psi : \Omega \rightarrow \text{Aut}(\tilde{\Gamma})$ be the homomorphism induced by φ . Note that H is mapped injectively into $\text{Aut}(\tilde{\Gamma})$ and that the image of H under that map coincides with $\psi(\Omega)$. The structure of Π as an Ω -group is given by a homomorphism $\kappa : \Omega \rightarrow \text{Aut}(\Pi)$. Let J denote the image of κ . Let $\lambda : \Omega \rightarrow \text{Aut}(\tilde{\Pi})$ be the homomorphism induced by κ . With this notation, we have $\tau \circ \psi(\alpha) = \lambda(\alpha) \circ \tau$ for all $\alpha \in \Omega$.

We will assume at first that τ is an isomorphism. Thus, τ induces an isomorphism from $\text{Aut}(\tilde{\Gamma})$ to $\text{Aut}(\tilde{\Pi})$ which sends $\psi(\Omega)$ to $\lambda(\Omega)$. Since J is mapped injectively into $\text{Aut}(\tilde{\Pi})$, it is clear that τ induces an isomorphism $H \rightarrow J$. Also, **BBT** implies that there is a continuous, surjective homomorphism $\delta : \Gamma \rightarrow \Pi$ such that $\tilde{\delta} = \tau$. Let $\Delta = \ker(\delta)$. Let $\text{Aut}(\Gamma, \Delta)$ denote the group of continuous automorphisms of Γ fixing the subgroup Δ . Thus, $\text{Aut}(\Gamma, \Delta)$ is a subgroup of $\text{Aut}(\Gamma)$ and we have a homomorphism

$$(2) \quad \text{Aut}(\Gamma, \Delta) \longrightarrow \text{Aut}(\Pi)$$

whose kernel N' is a subgroup of the kernel of (1) and hence is a pro- p subgroup of $\text{Aut}(\Gamma, \Delta)$. One also sees easily that (2) is surjective, just as for the map (1). Let G' denote the inverse image of J under (2). Thus, $G'/N' \cong J$. It follows from **SZT** that G' contains a subgroup H' such that $G' = H'N'$ and $H' \cap N' = \{id_{G'}\}$. It is clear that (2) maps H' isomorphically to J .

Moreover, the map $\kappa : \Omega \rightarrow J$ determines a map $\varphi' : \Omega \rightarrow H'$. If we regard Γ as an Ω -group by using the map φ' (instead of using φ), then δ becomes a surjective Ω -homomorphism from Γ to Π .

Note that φ and φ' induce the same map from Ω to $\text{Aut}(\tilde{\Gamma})$, namely the map ψ . As previously, let N be the kernel of (1) and let G be the inverse image of $\psi(\Omega)$. Then $H' \subset G$ and $G = H'N$. It follows from **SZT** that H and H' are conjugate subgroups of G . More precisely, there is an element $\eta \in N$ such that $H' = \eta H \eta^{-1}$. Consequently, if $\alpha \in \Omega$, then $\varphi'(\alpha) \circ \eta = \eta \circ \varphi(\alpha)$. Also, η induces the identity map on $\tilde{\Gamma}$.

The above remarks show that $\sigma = \delta \circ \eta$ is a surjective Ω -homomorphism from Γ to Π and that $\tilde{\sigma}$ coincides with the isomorphism τ from $\tilde{\Gamma}$ to $\tilde{\Pi}$. To complete the proof, suppose now that τ is not injective. Then one can define an isomorphism

$$\tau_1 : \tilde{\Gamma} \longrightarrow \tilde{\Pi} \times \ker(\tau)$$

of representation spaces for Ω such that composing τ_1 with projection to the factor $\tilde{\Pi}$ gives the map τ . Let $\Pi_1 = \Pi \times \ker(\tau)$. Thus, Π_1 is a pro- p Ω -group and the natural projection map from $\Pi_1 \rightarrow \Pi$ is a surjective Ω -homomorphism. Hence, as we have shown above, there is a surjective Ω -homomorphism σ_1 from Γ to Π_1 such that $\tilde{\sigma}_1 = \tau_1$. Composing with the projection map from Π_1 to Π gives a surjective Ω -homomorphism σ such that $\tilde{\sigma} = \tau$. ■

Remark 2.3.2. Proposition 2.1.1 is a consequence of proposition 2.3.1. If Ω satisfies assumption **A**, then we pointed out at the end of section 2.3 that one can construct a free pro- p Ω -group Γ with any specified Ω -type as a free product. The construction gives us a set of generators $\{\gamma_1, \dots, \gamma_n\}$ of Γ consisting of Ω -elements. If χ is a \mathbf{Z}_p^\times -valued character of Ω , then the number of distinguished generators which are χ -elements for Ω is $m_\chi(\tilde{\Gamma})$.

For any Π , we can construct $\tilde{\Gamma}$ so that Γ has the same Ω -type as Π . Furthermore, if we choose a basis $\{\tilde{\pi}_1, \dots, \tilde{\pi}_n\}$ of $\tilde{\Pi}$ -consisting of Ω -elements, and if we suitably modify the indexing for the γ_i 's, then we can choose $\tau : \tilde{\Gamma} \rightarrow \tilde{\Pi}$ so that $\tau(\tilde{\gamma}_i) = \tilde{\pi}_i$ for $1 \leq i \leq n$. If we choose a lifting σ of τ as in proposition 2.3.1, then $\pi_i = \sigma(\gamma_i)$ will be an Ω -element of Π whose image in $\tilde{\Pi}$ is $\tilde{\pi}_i$ for each i . ◇

Remark 2.3.3. This remark concerns the usual universal mapping property for a free pro- p group Γ on a finite set Σ . If one replaces Σ by another set of topological generators S which has the same cardinality as Σ , then the universal mapping property also holds for S and Γ . To justify this, first note that if $f : \Sigma \rightarrow S$ is a bijection, then the unique continuous homomorphism $\varphi : \Gamma \rightarrow \Gamma$ such that $\varphi|_\Sigma = f$ is a minimal presentation of Γ . Hence the number of relations is the \mathbf{F}_p -dimension of $H^2(\Gamma, \mathbf{F}_p)$, which is zero. Hence φ is also injective

and therefore is an isomorphism. The universal mapping property for the pair (Γ, S) follows from that same property for the pair (Γ, Σ) . \diamond

3 Properties of p -rational fields.

Suppose that K is a number field and that p is an odd prime. Let Σ_p be the set of primes of K lying above p . We define the following three extensions of K : M is the compositum of all finite p -extensions of K which are unramified outside of Σ_p , M^{ab} is the maximal abelian extension of K contained in M , and L is the compositum of all cyclic extensions of K of degree p which are contained in M . If we let Γ denote $\text{Gal}(M/K)$, then Γ is a pro- p group, $\Gamma^{ab} \cong \text{Gal}(M^{ab}/K)$ is the maximal, abelian quotient of Γ , and the Frattini quotient $\tilde{\Gamma}$ can be identified with $\text{Gal}(L/K)$. If it is needed to avoid confusion, we will include a subscript K , writing M_K instead of M , Γ_K^{ab} instead of Γ^{ab} , etc.

We can consider Γ^{ab} as a \mathbf{Z}_p -module. It is known to be finitely-generated. The Frattini quotients of Γ and Γ^{ab} are the same and that gives the first of the following inequalities:

$$(3) \quad \dim_{\mathbf{F}_p}(\tilde{\Gamma}) \geq \text{rank}_{\mathbf{Z}_p}(\Gamma^{ab}) \geq r_2(K) + 1$$

Here $r_2(K)$ denotes the number of complex primes of K . The second inequality is a well-known result. (See [Was], section 13.5, for example.) Let $r_1(K)$ denote the number of real primes of K . If K/\mathbf{Q} is Galois, then there are two possibilities: Either $r_1(K) = 0$, $r_2(K) = \frac{1}{2}[K : \mathbf{Q}]$ (the totally complex case) or $r_1(K) = [K : \mathbf{Q}]$, $r_2(K) = 0$ (the totally real case).

A number field K is said to be “ p -rational” if $\dim_{\mathbf{F}_p}(\tilde{\Gamma}) = r_2(K) + 1$. The simplest example is $K = \mathbf{Q}$. One can show by class field theory (or by using the Kronecker-Weber theorem) that $M = \mathbf{Q}_\infty$, the cyclotomic \mathbf{Z}_p -extension of \mathbf{Q} . In general, a number field K is p -rational if and only if the following two requirements are satisfied:

- (i) $\text{rank}_{\mathbf{Z}_p}(\Gamma^{ab}) = r_2(K) + 1$,
- (ii) Γ^{ab} is torsion-free as a \mathbf{Z}_p -module.

The first statement is Leopoldt’s conjecture for K and p . It is known to hold when K is an abelian extensions of \mathbf{Q} and p is any prime. In principle, one can check the second requirement by using class field theory. We will discuss this for various types of number fields in section 4.

Consider the special case where K is totally real. Then K is p -rational if and only if $M^{ab} = K\mathbf{Q}_\infty$, the cyclotomic \mathbf{Z}_p -extension of K . It then follows from **BBT** that Γ has one topological generator and therefore that Γ is abelian. Thus, $\Gamma = \Gamma^{ab} \cong \mathbf{Z}_p$, a free pro- p

group on one generator. That is, a totally real number field K will be p -rational if and only if $M = K\mathbf{Q}_\infty$.

3.1. Freeness. The importance of p -rationality for us is contained in the following result which is proved in [MoNg]. The conclusion is one of their equivalent statements about p -rationality. It will be useful to give an argument here.

Proposition 3.1.1. *If K is p -rational, then Γ is a free pro- p group on $r_2(K) + 1$ generators.*

Proof. We have already explained this result if $r_2(K) = 0$. In general, it turns out to be a consequence of the fact that the global Euler-Poincaré characteristic for the trivial $\text{Gal}(K_\Sigma/K)$ -module $\mathbf{Z}/p\mathbf{Z}$ is equal to $-r_2(K)$. Here Σ consists of the primes lying over p or ∞ and K_Σ is the maximal extension of K unramified outside of Σ . We obviously have $\dim_{\mathbf{F}_p}(H^0(K_\Sigma/K, \mathbf{Z}/p\mathbf{Z})) = 1$. Assuming that K is p -rational, we have

$$\dim_{\mathbf{F}_p}(H^1(K_\Sigma/K, \mathbf{Z}/p\mathbf{Z})) = \dim_{\mathbf{F}_p}(H^1(\Gamma, \mathbf{Z}/p\mathbf{Z})) = r_2(K) + 1$$

Using the Euler-Poincaré characteristic, it follows that $\dim_{\mathbf{F}_p}(H^2(K_\Sigma/K, \mathbf{Z}/p\mathbf{Z})) = 0$. Furthermore, by definition, M has no nontrivial Galois p -extension contained in K_Σ . A result of Neumann (corollary 10.4.3 in [NSW]) implies that $H^i(K_\Sigma/M, \mathbf{Z}/p\mathbf{Z}) = 0$ for all $i \geq 1$. Using this result just for $i = 1$, it follows that the inflation map

$$H^2(\Gamma, \mathbf{Z}/p\mathbf{Z}) \longrightarrow H^2(K_\Sigma/K, \mathbf{Z}/p\mathbf{Z})$$

is injective and therefore that $H^2(\Gamma, \mathbf{Z}/p\mathbf{Z}) = 0$. It follows that Γ has a minimal presentation with $r_2(K) + 1$ generators and no relations, proving the stated result. ■

Note that the converse of proposition 3.1.1 is clearly true. In fact, one has the following stronger statement: *If Γ is a free pro- p group, then K is p -rational.* To see this, note that the vanishing of $H^i(K_\Sigma/M, \mathbf{Z}/p\mathbf{Z})$ for $i = 1$ and $i = 2$ implies that the inflation map $H^i(\Gamma, \mathbf{Z}/p\mathbf{Z}) \rightarrow H^i(K_\Sigma/K, \mathbf{Z}/p\mathbf{Z})$ is an isomorphism, not just for $i = 1$ (which is obvious), but for $i = 2$ too. This follows from proposition 1.6.6 in [NSW]. Hence the Euler-Poincaré characteristic of $\mathbf{Z}/p\mathbf{Z}$ as a Γ -module is also equal to $-r_2(K)$. In particular, if Γ is a free pro- p group, then $H^2(\Gamma, \mathbf{Z}/p\mathbf{Z}) = 0$ and hence the \mathbf{F}_p -dimension of $H^1(\Gamma, \mathbf{Z}/p\mathbf{Z})$ is $r_2(K) + 1$. Therefore, Γ indeed has a topological generating set of that cardinality.

Remark 3.1.2. There is a considerable literature concerning p -rational fields, including [Ngu], [JaNg], [Mov], and [MoNg]. One additional equivalent statement which is found in

those references (e.g., proposition 2 in [Mov]) involves the subgroup $\mathcal{H}_p(K)$ of K^\times consisting of p -hyperprimary elements. An element $\alpha \in K^\times$ is said to be “ p -hyperprimary” if $\alpha\mathcal{O}_K = \mathfrak{a}^p$ for some fractional ideal \mathfrak{a} of K and if $\alpha \in (K_v^\times)^p$ for all primes v of K lying above p . Then K is p -rational if and only if the following two statements are satisfied:

- (a) The map $\mu(K)_p \longrightarrow \prod_{v \in \Sigma_p} \mu(K_v)_p$ is an isomorphism.
- (b) $\mathcal{H}_p(K) = (K^\times)^p$.

In statement (a), $\mu(K)_p$ and $\mu(K_v)_p$ denote the groups of p -power roots of unity in the specified fields. It is obviously satisfied if $\mu_p \not\subset K_v$ for all $v|p$. If the class number of K is not divisible by p , then statement (b) means that if a unit α of K is a p -th power in the completions K_v for all $v \in \Sigma_p$, then α is a p -th power in K itself. \diamond

If K fails to be p -rational, it might still be useful to know if there exists a Galois extension N of K such that $\text{Gal}(N/K)$ is a free pro- p group on r generators for some reasonably large value of r . For our purpose, we would also want N to be Galois over \mathbf{Q} . Very little is known about this question. Some comments can be found in [Yam] and [Hub].

3.2. The Ω -type of $\Gamma = \text{Gal}(M/K)$. Assume now that K is Galois over \mathbf{Q} and let $\Omega = \text{Gal}(K/\mathbf{Q})$. It is clear that $M = M_K$ will also be Galois over \mathbf{Q} . We then have an exact sequence:

$$(4) \quad 1 \longrightarrow \Gamma \longrightarrow \text{Gal}(M/\mathbf{Q}) \longrightarrow \Omega \longrightarrow 1 .$$

We will assume from now on that K is totally complex. If $K \rightarrow \mathbf{C}$ is a field embedding, then the restriction of complex conjugation to K is an element of order 2. We let Ω_∞ denote the subgroup that it generates. It may depend on the embedding, but the choice won't matter.

There is a well-defined action of Ω on Γ^{ab} . The next result is valid even if Ω has order divisible by p . We let χ_0 denote the trivial representation of Ω .

Proposition 3.2.1. *Assume that K is a totally complex Galois extension of \mathbf{Q} and that Leopoldt's conjecture holds for K and p . Let ε_1 denote the nontrivial character of Ω_∞ . Then*

$$\Gamma^{ab} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \cong \text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1) \oplus \chi_0$$

as representations spaces for Ω .

Proof. The argument is based on class field theory. Let $V = \Gamma^{ab} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Note that V is a \mathbf{Q}_p -representation space for Ω of dimension $r_2(K) + 1$ since we assume that Leopoldt's conjecture holds for K and p . Let E denote the group of units of K . Then $W = E \otimes_{\mathbf{Z}} \mathbf{Q}_p$ is

another \mathbf{Q}_p -representation space for Ω . Its dimension is $[K : \mathbf{Q}] - 1$ if K is real, $\frac{1}{2}[K : \mathbf{Q}] - 1$ if K is complex. It is well-known that

$$W \oplus \chi_0 \cong \text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_0)$$

as representation spaces for Ω , where ε_0 is the trivial character of Ω_∞ . This can be deduced from the usual proof of Dirichlet's unit theorem. If we replace E by a subgroup E' of finite index, then $E' \otimes_{\mathbf{Z}} \mathbf{Q}_p$ defines an isomorphic representation space for Ω .

Let $\mathcal{K} = K \otimes_{\mathbf{Q}} \mathbf{Q}_p$. We can identify \mathcal{K} with the product of the completions of K at the primes above p . Let \mathcal{U} be the product of the local unit groups in the completions. Thus, \mathcal{U} is a compact subgroup of \mathcal{K}^\times . Let \mathcal{U}' denote the maximal pro- p subgroup of \mathcal{U} , which has finite index in \mathcal{U} . Then \mathcal{U}' can be regarded as a \mathbf{Z}_p -module. The log maps for the completions of K at the primes above p define a \mathbf{Z}_p -module homomorphism $\log_{\mathcal{U}'}$ from \mathcal{U}' to \mathcal{K} with finite kernel and open image. Now Ω acts on \mathcal{K} as a group of \mathbf{Q}_p -algebra automorphisms. Regarding \mathcal{K} as a \mathbf{Q}_p -representation space for Ω , it is isomorphic to the regular representation. The action of Ω on the multiplicative group of \mathcal{K} induces an action of Ω on \mathcal{U}' . Furthermore, $\log_{\mathcal{U}'}$ is Ω -equivariant. It follows that the \mathbf{Q}_p -representation space $U = \mathcal{U}' \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ for Ω is isomorphic to the regular representation.

There is a canonical embedding $E \rightarrow \mathcal{U}$. Let E' denote the maximal subgroup of E which is mapped into \mathcal{U}' by that embedding. For simplicity, we identify E' with its image in \mathcal{U}' . Then we get an induced map of $E' \otimes_{\mathbf{Z}} \mathbf{Z}_p \rightarrow \mathcal{U}'$ and the image of that map is the closure $\overline{E'}$ of E' in \mathcal{U}' . Since Leopoldt's conjecture is assumed to hold for K and p , the \mathbf{Z}_p -ranks of $E' \otimes_{\mathbf{Z}} \mathbf{Z}_p$ and $\overline{E'}$ are equal and therefore the kernel of the map $E' \otimes_{\mathbf{Z}} \mathbf{Z}_p \rightarrow \overline{E'}$ is finite. It follows that the representation spaces $E' \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and $\overline{E'} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ for Ω are isomorphic.

Class field theory defines a homomorphism

$$\mathcal{U}' / \overline{E'} \longrightarrow \Gamma^{ab}$$

which has finite kernel and cokernel. Tensoring those \mathbf{Z}_p -modules with \mathbf{Q}_p defines an isomorphism of \mathbf{Q}_p -representation spaces for Ω . It follows that $U/W \cong V$. We have already discussed the structure of $E' \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, which is isomorphic to W , and of $U = \mathcal{U}' \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. The regular representation of Ω_∞ is isomorphic to $\varepsilon_0 \oplus \varepsilon_1$ and hence

$$U \cong \text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_0) \oplus \text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1) \quad .$$

The stated isomorphism for V follows from the above isomorphisms for W and U . ■

Assume that Ω satisfies assumption **B**. The Schur-Zassenhaus theorem then implies that the exact sequence (4) splits and hence that there exists a splitting homomorphism from Ω

to $\text{Gal}(M/\mathbf{Q})$. It is not unique, but we will fix one choice. Thus, Ω can be identified with a subgroup of $\text{Gal}(M/\mathbf{Q})$. Conjugation by elements of Ω then defines an action of Ω on Γ , and hence Γ becomes an Ω -group. One sees easily that the Ω -type of Γ does not depend on the choice of splitting homomorphism. If one assumes that K is p -rational, then Γ is a free Ω -group. As mentioned in remark 2.2.1, its Ω -type is then determined by the representation space $V = \Gamma^{ab} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ for Ω . However, if K is not p -rational, then the \mathbf{Z}_p -torsion submodule of Γ^{ab} will be nontrivial and will make an additional contribution to the Ω -type of Γ .

If K is a totally complex, abelian extension of \mathbf{Q} and $\chi \in \widehat{\Omega}$, then we say that χ is odd if $\chi|_{\Omega_\infty} = \varepsilon_1$. Let $\widehat{\Omega}_{\text{odd}}$ denote the set of *odd* characters of Ω . The following corollary determines the Ω -type of Γ completely under the stated assumptions. It follows directly from remark 2.2.1 and proposition 3.2.1.

Corollary 3.2.2. *Suppose that K is totally complex and p -rational. Suppose that Ω satisfies assumption **A**. Then $m_\chi(\widetilde{\Gamma}) = 1$ for all $\chi \in \widehat{\Omega}_{\text{odd}} \cup \{\chi_0\}$ and $m_\chi(\widetilde{\Gamma}) = 0$ for all other χ 's in $\widehat{\Omega}$. These multiplicities determine the Ω -type of Γ .*

Remark 3.2.3. If Ω_∞ is a normal subgroup of Ω , then K^{Ω_∞} is the maximal totally real subfield of K and K is a so-called CM field. As above, we let $V = \Gamma^{ab} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. One has a decomposition $V = V^{(\varepsilon_0)} \oplus V^{(\varepsilon_1)}$ for the action of Ω_∞ . Even without assuming the validity of Leopoldt's conjecture, the above proof shows that

$$V^{(\varepsilon_1)} \cong \text{Ind}_{\Omega_\infty}^{\Omega}(\varepsilon_1)$$

as representation spaces for Ω . If one doesn't assume that Ω_∞ is normal, then the proof shows that $\text{Ind}_{\Omega_\infty}^{\Omega}(\varepsilon_1) \oplus \chi_0$ is a direct summand in V as a representation space for Ω .

We can also say something about $\widetilde{\Gamma}$ as an \mathbf{F}_p -representation space in the case where Ω has order prime to p . Assume that K is totally complex. For brevity, let γ and ξ denote the \mathbf{Q}_p -representations of Ω defined by V and by $\text{Ind}_{\Omega_\infty}^{\Omega}(\varepsilon_1) \oplus \chi_0$, respectively. Since ξ is a direct summand in γ , and Ω has order prime to p , it follows from remark 2.2.1 that $\bar{\xi}$ is a direct summand in $\bar{\gamma}$. Furthermore, if $\Gamma[p]$ denotes the maximal subgroup of Γ of exponent p , then $\widetilde{\Gamma} \cong \bar{\gamma} \oplus \Gamma[p]$ as \mathbf{F}_p -representations spaces for Ω . Therefore, it follows that $\bar{\xi}$ is a direct summand in $\widetilde{\Gamma}$. \diamond

3.3. Criteria involving subfields. Assume that K/\mathbf{Q} is a finite, abelian extension and that Ω has order prime to p , but not necessarily exponent dividing $p-1$. Let $\text{Irr}_{\mathbf{Q}_p}(\Omega)$ denote the set of irreducible representations of Ω over \mathbf{Q}_p , up to isomorphism. If $\chi \in \text{Irr}_{\mathbf{Q}_p}(\Omega)$, we denote its degree by $n(\chi)$. Let F_χ be the fixed field for $\ker(\chi)$. Then F_χ is a cyclic extension of \mathbf{Q} . Note that $n(\chi) = 1$ if and only if $[F_\chi : \mathbf{Q}]$ divides $p-1$. Also, if F is any extension of

\mathbf{Q} contained in K , then $F_\chi \subseteq F$ if and only if χ factors through $\text{Gal}(F/\mathbf{Q})$. If F/\mathbf{Q} is cyclic, then there exists at least one $\chi \in \text{Irr}_{\mathbf{Q}_p}(\Omega)$ such that $F_\chi = F$.

We have the following canonical decomposition, where we let $e_\chi \in \mathbf{Z}_p[\Omega]$ denote the idempotent for χ and where our notation now includes a subscript indicating the field.

$$\Gamma_K^{ab} \cong \bigoplus_{\chi} (\Gamma_K^{ab})^{e_\chi} .$$

as $\mathbf{Z}_p[\Omega]$ -modules, where χ varies over $\text{Irr}_{\mathbf{Q}_p}(\Omega)$ in the above direct sum. Furthermore, if F is any subfield of K , cyclic or not, then Γ_F^{ab} can be identified with the maximal quotient of Γ_K^{ab} on which $\text{Gal}(K/F)$ acts trivially. Hence, we have the following isomorphism

$$\Gamma_F^{ab} = \text{Gal}(M_F^{ab}/F) \cong \bigoplus_{F_\chi \subseteq F} (\Gamma_K^{ab})^{e_\chi}$$

where the notation indicates that χ varies over the elements of $\text{Irr}_{\mathbf{Q}_p}(\Omega)$ such that $F_\chi \subseteq F$. In particular, taking $F = \mathbf{Q}$, we have $M_{\mathbf{Q}}^{ab} = \mathbf{Q}_\infty$, the cyclotomic \mathbf{Z}_p -extension of \mathbf{Q} . This is so because p is odd. Thus, we have $(\Gamma_K^{ab})^{e_{\chi_0}} \cong \text{Gal}(\mathbf{Q}_\infty/\mathbf{Q}) \cong \mathbf{Z}_p$, where χ_0 denotes the trivial character. \diamond

The above remark gives a proof of the following proposition. One just observes that Γ_K^{ab} is torsion-free if and only if $(\Gamma_K^{ab})^{e_\chi}$ is torsion-free for all $\chi \in \widehat{\Omega}$.

Proposition 3.3.1. *If K is a finite abelian extension of \mathbf{Q} and $[K : \mathbf{Q}]$ is not divisible by p , then K is p -rational if and only if every cyclic extension of \mathbf{Q} contained in K is p -rational.*

Remark 3.3.2. Let us assume that K satisfies assumption **A**, but not necessarily that K is p -rational. We let $\widehat{\Omega}_{\text{odd}}$ denote the set of odd characters of Ω , which we can regard as characters with values in \mathbf{Z}_p^\times . They can also be regarded as irreducible representations for Ω over \mathbf{Q}_p . Remark 3.2.3 implies that the \mathbf{Z}_p -rank of $(\Gamma_K^{ab})^{e_\chi}$ is equal to 1 if $\chi \in \widehat{\Omega}_{\text{odd}} \cup \{\chi_0\}$. Thus, for every such χ , there exists a uniquely determined Galois extension $K_\infty^{(\chi)}$ of K with the following properties: $\text{Gal}(K_\infty^{(\chi)}/K) \cong \mathbf{Z}_p$, $K_\infty^{(\chi)}$ is Galois over \mathbf{Q} , and Ω acts on $\text{Gal}(K_\infty^{(\chi)}/K)$ by the character χ . The field $K_\infty^{(\chi)}$ is a \mathbf{Z}_p -extension of K . Using the notation of section 2, we have $\text{Gal}(K_\infty^{(\chi)}/\mathbf{Q}) \cong \Gamma_\chi \rtimes \Omega$. Note that $K_\infty^{(\chi_0)} = K\mathbf{Q}_\infty$, the cyclotomic \mathbf{Z}_p -extension of K . The field M_K^{ab} is a finite extension of the compositum of the $K_\infty^{(\chi)}$'s. The field K will be p -rational if and only if M_K^{ab} coincides with that compositum. \diamond

We will mention without proof a criterion which requires only assumption **B** for Ω . If T is a collection of subgroups of Ω , then we say that T is “*ample*” if the following property holds: *For every \mathbf{Q}_p -irreducible representation χ of Ω , $\mathbf{1}_\Theta$ is a constituent in $\chi|_\Theta$ for at least one $\Theta \in T$.* Here $\mathbf{1}_\Theta$ denotes the trivial representation of Θ . Equivalently, one can make the same requirement on the restrictions $\chi|_\Theta$, where χ varies over all the absolutely irreducible representations of Ω . If F is any subfield of K , let $\Theta_F = \text{Gal}(K/F)$. A collection \mathcal{F} of subfields of K is said to be ample if the corresponding collection of subgroups $\{\Theta_F\}_{F \in \mathcal{F}}$ is ample. The proof of the next result is somewhat similar to the proof of proposition 3.3.1. It is not difficult if K is totally real. If K is totally complex, then remark 3.2.3 is useful as well as the following easily proved fact:

$$\dim_{\mathbf{Q}_p}(\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_\infty)^{\Theta_F}) = r_2(F)$$

for every subfield F of K . If Ω is abelian, then the collection \mathcal{F} consisting of all cyclic extensions of \mathbf{Q} contained in K will obviously be ample. Thus, the following result is a generalization of proposition 3.3.1.

Proposition 3.3.3. *Suppose that K/\mathbf{Q} is a finite Galois extension and that \mathcal{F} is an ample collection of subfields of K . Suppose that p is a prime and that $[K : \mathbf{Q}]$ is not divisible by p . Then K is p -rational if and only if every field F in \mathcal{F} is p -rational.*

As one simple illustration, suppose that $\text{Gal}(K/\mathbf{Q}) \cong S_3$ and that $p > 3$. One can take \mathcal{F} to consist of the quadratic subfield and any cubic subfield of K . One sees easily that \mathcal{F} is ample.

4 Examples of abelian p -rational fields.

We continue to assume that p is an odd prime. We describe a variety of examples of p -rational fields which will be useful in the construction in section 6. We have already mentioned the simple example $K = \mathbf{Q}$ for which we have $M_{\mathbf{Q}}^{ab} = \mathbf{Q}_\infty$, the cyclotomic \mathbf{Z}_p -extension of \mathbf{Q} .

4.1. Quadratic fields. Suppose that $[K : \mathbf{Q}] = 2$. Then $\widehat{\Omega} = \{\chi_0, \chi_1\}$, where χ_0 is the trivial character and χ_1 is of order 2. If K is complex, then χ_1 is odd and the field $K_\infty^{(\chi_1)}$ defined in remark 3.3.2 is usually called the anticyclotomic \mathbf{Z}_p -extension of K . The field $K_\infty^{(\chi_0)}$ is just $K\mathbf{Q}_\infty$, the cyclotomic \mathbf{Z}_p -extension of K . Let h_K denote the class number of K . The following result is not entirely new. Very similar results are proved in [Fuj] and in [Min] if K is complex. For simplicity, we make an assumption about p which guarantees that $\mu_p \not\subset K_v$ for the primes(s) v of K lying over p .

Proposition 4.1.1. *Suppose that K is a quadratic field and that either $p \geq 5$ or that $p = 3$ and is unramified in K/\mathbf{Q} .*

(i) *Assume that K is complex. Then K is p -rational if and only if the p -Hilbert class field of K is contained in $K_\infty^{(\chi_1)}$. In particular, if h_K is not divisible by p , then K is p -rational.*

(ii) *Assume that K is real. Then K is p -rational if and only if h_K is not divisible by p and the fundamental unit ε_0 of K is not a p -th power in the completion K_v , where v is a prime of K lying above p .*

Proof. The field K will be p -rational if and only if $(\Gamma_K^{ab})^{e_{\chi_1}}$ is torsion-free. We will let $(\Gamma_K^{ab})_{tors}^{e_{\chi_1}}$ denote the torsion-subgroup of $(\Gamma_K^{ab})^{e_{\chi_1}}$. The assumption about p guarantees that the completion K_v at a prime $v|p$ doesn't contain μ_p , the group of p -th roots of unity. In the notation of the proof of proposition 3.2.1, one then has $(\mathcal{U}')^{e_{\chi_1}} \cong \mathbf{Z}_p$.

If K is complex, then class field theory gives an exact sequence

$$1 \longrightarrow (\mathcal{U}')^{e_{\chi_1}} \longrightarrow (\Gamma_K^{ab})^{e_{\chi_1}} \longrightarrow \text{Gal}(H/K) \longrightarrow 1 ,$$

where H denotes the p -Hilbert class field of K . The image of $(\mathcal{U}')^{e_{\chi_1}}$ in $(\Gamma_K^{ab})^{e_{\chi_1}}$ is just the inertia subgroup for the prime(s) v dividing p . The surjectivity of the map to $\text{Gal}(H/K)$ follows from the fact that $\Omega = \text{Gal}(K/\mathbf{Q})$ acts on $\text{Gal}(H/K)$ by χ_1 . It follows that $(\Gamma_K^{ab})_{tors}^{e_{\chi_1}}$ is mapped injectively into $\text{Gal}(H/K)$ under the restriction map. That image will be $\text{Gal}(H/H')$, where H' is an extension of K contained in H . Furthermore, the fixed field for $(\Gamma_K^{ab})_{tors}^{e_{\chi_1}}$ is precisely $K_\infty^{(\chi_1)}$. Consequently, $H' = H \cap K_\infty^{(\chi_1)}$. This shows that $(\Gamma_K^{ab})^{e_{\chi_1}}$ is torsion-free if and only if $H \subset K_\infty^{(\chi_1)}$.

Now assume that K is real. There is a power $\varepsilon = \varepsilon_0^a$, where a is not divisible by p , such that $\varepsilon \in \mathcal{U}'$. We can choose a to be even so that ε has norm 1. Then $\varepsilon \in (\mathcal{U}')^{e_{\chi_1}}$ and we have an exact sequence

$$1 \longrightarrow (\mathcal{U}')^{e_{\chi_1}} / \langle \varepsilon \rangle \longrightarrow (\Gamma_K^{ab})^{e_{\chi_1}} \longrightarrow \text{Gal}(H/K) \longrightarrow 1 .$$

Thus, $(\Gamma_K^{ab})^{e_{\chi_1}}$ is finite if K is real. It follows that K is p -rational if and only if both $(\mathcal{U}')^{e_{\chi_1}} / \langle \varepsilon \rangle$ and $\text{Gal}(H/K)$ are trivial. The first group is nontrivial if and only if ε is a p -th power in $(\mathcal{U}')^{e_{\chi_1}}$, or equivalently, if and only if ε_0 is a p -th power in K_v for $v|p$. The group $\text{Gal}(H/K)$ is nontrivial if and only if h_K is divisible by p . ■

The following corollaries deal with various special cases. The first two concern $p = 3$ and $p = 5$.

Corollary 4.1.2. *Suppose that $K = \mathbf{Q}(\sqrt{d})$, where d is a squarefree integer and $3 \nmid d$. Then K is 3-rational if and only if the class number of $\mathbf{Q}(\sqrt{-3d})$ is not divisible by 3.*

The same criterion is also proved by Fujii in [Fuj] (theorem 4.1) and by Minardi in [Min] (the corollary to proposition 6.B) when $d < 0$. One can weaken the assumption that $3 \nmid d$. It suffices to assume that μ_3 is not contained in the completion K_v of K at a prime v dividing 3.

Proof. Take $p = 3$. Let $L^{(\chi_1)}$ be the fixed field for the Frattini subgroup of $(\Gamma_K^{ab})^{e_{\chi_1}}$. Thus, $L^{(\chi_1)}$ is Galois over \mathbf{Q} , $\text{Gal}(L^{(\chi_1)}/K)$ is an abelian group of exponent 3, and $\text{Gal}(K/\mathbf{Q})$ acts on $\text{Gal}(L^{(\chi_1)}/K)$ by χ_1 . If K is complex, then $L^{(\chi_1)}$ contains the first layer $K_1^{(\chi_1)}$ in the anticyclotomic \mathbf{Z}_3 -extension $K_\infty^{(\chi_1)}/K$, which is a cyclic extension of K of degree 3. In that case, the field K is 3-rational if and only if $L^{(\chi_1)} = K_1^{(\chi_1)}$. If K is real, then K is 3-rational if and only if $L^{(\chi_1)} = K$.

We will use the reflection principle. We assume that $d \neq 1$ so that $[K : \mathbf{Q}] = 2$. Let $J = K(\mu_3) = \mathbf{Q}(\sqrt{d}, \sqrt{-3d})$ and let $F = \mathbf{Q}(\sqrt{-3d})$. Then a Kummer theory argument shows that $JL^{(\chi_1)}$ is a compositum of fields of the form $J(\sqrt[3]{\alpha})$, where $\alpha \in F^\times$ and $N_{F/\mathbf{Q}}(\alpha) = 1$. Since $3 \nmid d$, it is clear that 3 is ramified in F/\mathbf{Q} . It follows that $\text{ord}_v(\alpha) = 0$ for the prime v of F lying over 3. Furthermore, the fact that $L^{(\chi_1)}/K$ is unramified at primes v not lying over 3 implies that $\text{ord}_v(\alpha) \equiv 0 \pmod{3}$ for all such v . Thus, $(\alpha) = \mathfrak{a}^3$, where \mathfrak{a} is a fractional ideal of F .

Assume that the class number of F is not divisible by 3. Then \mathfrak{a} is principal. Thus $\alpha = \beta^3 \varepsilon$, where $\beta \in F^\times$ and ε is a unit of F . Thus, $J(\sqrt[3]{\alpha}) = J(\sqrt[3]{\varepsilon})$. If K is real, then F is complex and ε is a root of unity whose order is not divisible by 3 (because $d \neq 1$). Thus, $J(\sqrt[3]{\varepsilon}) = J$ and hence $L^{(\chi_1)} = K$. If K is complex, then F is real and $\pm \varepsilon$ is a power of the fundamental unit of F . Hence $J(\sqrt[3]{\varepsilon})$ is a cyclic extension of J . It follows that $L^{(\chi_1)}/K$ is cyclic and consequently we must have $L^{(\chi_1)} = K_1^{(\chi_1)}$. In both cases, we see that K is indeed 3-rational.

Conversely, assume that the class number of F is divisible by 3. Let c be an ideal class of order 3. Then $\text{Gal}(K/\mathbf{Q})$ acts on c by χ_1 . One verifies easily that one can choose an ideal $\mathfrak{a} \in c$ so that $\text{Gal}(K/\mathbf{Q})$ acts on \mathfrak{a} by χ_1 and that \mathfrak{a}^3 has a generator α such that $N_{K/\mathbf{Q}}(\alpha) = 1$. Furthermore, $J(\sqrt[3]{\alpha})/J$ has degree 3 and is unramified except at 3. It follows that $JL^{(\chi_1)}$ contains $J(\sqrt[3]{\alpha})$. If K is real, then it follows that $L^{(\chi_1)} \neq K$ and therefore K is not 3-rational. Now assume that K is complex. Then F is real and $JL^{(\chi_1)}$ also contains $J(\sqrt[3]{\varepsilon_0})$, where ε_0 is the fundamental unit of F . It follows that $JL^{(\chi_1)}/J$ is not cyclic and hence $L^{(\chi_1)}$ is not a cyclic extension of K . This means that K is not 3-rational. ■

Remark 4.1.3. A similar argument gives the following generalization for an arbitrary odd prime p . We assume that $K = \mathbf{Q}(\sqrt{d})$ and that $p \nmid d$. Let $J = K(\mu_p)$ and let A denote the maximal elementary abelian p -subgroup of the ideal class group of J . We regard A as

an \mathbf{F}_p -representation space for $\text{Gal}(J/\mathbf{Q})$. The action of $\text{Gal}(J/\mathbf{Q})$ on μ_p is described by a character $\omega : \text{Gal}(J/\mathbf{Q}) \rightarrow \mathbf{F}_p^\times$. We regard χ_1 as an \mathbf{F}_p^\times -valued character of $\text{Gal}(J/\mathbf{Q})$ too. Then the field K is p -rational if and only if the $\omega\chi_1$ -component $e_{\omega\chi_1}A$ of A is trivial. \diamond

Corollary 4.1.4. *Suppose that $K = \mathbf{Q}(\sqrt{d})$, where d is squarefree and $d > 1$. Assume that $d \equiv \pm 1 \pmod{5}$. Let $\varepsilon_0 = a_0 + b_0\sqrt{d}$ be the fundamental unit of K , where $a_0, b_0 \in \mathbf{Q}$ and have denominator 1 or 2. Then $\text{ord}_5(a_0b_0) \geq 1$. The field K is 5-rational if and only if $5 \nmid h_K$ and $\text{ord}_5(a_0b_0) = 1$.*

Proof. The congruence for d means that 5 splits in K/\mathbf{Q} . The fact that either a_0 or b_0 is divisible by 5, but not both, follows from the equation $a_0^2 - b_0^2d = \pm 1$ and the congruence for d . Divisibility refers to the ring $\mathbf{Z}[\frac{1}{2}]$. If \mathfrak{p} is either one of the two primes of K dividing 5, then $\varepsilon_0^2 \equiv \pm 1 \pmod{\mathfrak{p}}$. It is clear that ε_0 is a 5-th power in $K_{\mathfrak{p}}$ if and only if $\varepsilon_0^2 \equiv \pm 1 \pmod{\mathfrak{p}^2}$. Furthermore, it is not difficult to show $\varepsilon_0^2 \equiv \pm 1 \pmod{\mathfrak{p}^2}$ if and only if a_0 or b_0 is divisible by 5^2 . The stated result then follows from proposition 4.1.1. \blacksquare

Corollary 4.1.5. *Let $K = \mathbf{Q}(\sqrt{5})$. Suppose that p is an odd prime and $p \neq 5$. We will let $q = p$ if $p \equiv \pm 1 \pmod{5}$ and $q = p^2$ if $p \equiv \pm 2 \pmod{5}$. Then K is p -rational if and only if $F_q \not\equiv 1 \pmod{p^2}$, where F_q is the q -th Fibonacci number.*

Proof. Since $h_K = 1$, it follows that K is p -rational if and only if the fundamental unit ε_0 is not a p -th power in the completion of K at a prime \mathfrak{p} above p . Let F_n denote the n -th Fibonacci number. One has a well-known formula $F_n = a\varepsilon_0^{n-1} + b\bar{\varepsilon}_0^{n-1}$ for all $n \geq 1$, where $a, b \in K$ and $\bar{\varepsilon}$ is the conjugate of ε in K . We have $\sqrt{5}a = \varepsilon_0$ and $\sqrt{5}b = -\bar{\varepsilon}_0$. Thus, a and b are units in $K_{\mathfrak{p}}$. Now $\varepsilon_0^{q-1} \equiv 1 \pmod{\mathfrak{p}}$ and ε_0 is a p -th power in $K_{\mathfrak{p}}$ if and only if $\varepsilon_0^{q-1} \equiv 1 \pmod{\mathfrak{p}^2}$. Since $\bar{\varepsilon}_0 = -\varepsilon_0^{-1}$, the above congruences for ε_0 give similar congruences for $\bar{\varepsilon}_0$. It follows that $F_q \equiv 1 \pmod{p}$ and that ε_0 is a p -th power in $K_{\mathfrak{p}}$ if and only if $F_q \equiv 1 \pmod{p^2}$, proving the stated result. \blacksquare

Corollary 4.1.6. *Suppose that K is an imaginary quadratic field, that p satisfies the hypothesis in proposition 4.1.1, that the class number of K is divisible by p , and that the p -primary subgroup of the ideal class group of K is cyclic. Suppose that \mathfrak{a} is a fractional ideal of K whose ideal class has order p and that α is a generator of \mathfrak{a}^p . Then K is p -rational if and only if α is not a p -th power in K_v for a prime v of K lying above p .*

One can find this result in [Min], proposition 6.A. Note that if the p -primary subgroup of the class group of K is not cyclic, then proposition 4.1.1 clearly implies that K is not p -rational.

Proof. We will use the criterion in remark 3.1.1. The unit group of K is finite and of order prime to p . Furthermore, $N_{K/\mathbf{Q}}(\alpha)$ is a p -th power in \mathbf{Q} . If there are two primes of K above p and if α is a p -th power in the completion of K for one of those primes v , then α is also a p -th power in the completion at the other prime above p . The assumptions imply that if $\beta \in \mathcal{H}_p(K)$, the group of hyperprimary elements of K , then $\beta = \alpha^i \gamma^p$, where $\gamma \in K^\times$ and $0 \leq i < p$. Furthermore, by definition, β is a p -th power in K_v for all $v|p$. The assumption about p implies that $\mu(K_v)$ is trivial for $v|p$. Now if α is not a p -th power in K_v for $v|p$, then $i = 0$. Thus, it follows that $\mathcal{H}_p(K) = (K^\times)^p$ and hence that K is p -rational. For the converse, note that $\alpha \notin (K^\times)^p$ and that if α is a p -th power in K_v for a prime $v|p$, then $\alpha \in \mathcal{H}_p(K)$. ■

Remark 4.1.7. Suppose that K is an imaginary quadratic field and that the hypothesis in proposition 4.1.1 concerning the prime p is satisfied. Let A denote the p -primary subgroup of the ideal class group of K . The Artin map defines an isomorphism $A \rightarrow \text{Gal}(H/K)$, where H is the p -Hilbert class field of K . Let $H' = H \cap K_\infty^{(\chi_1)}$. Let B denote the inverse image of $\text{Gal}(H/H')$ under the Artin map. Just as in the proof of part (a) of proposition 4.1.1, one sees that the restriction map gives an isomorphism of the torsion subgroup of Γ_K^{ab} to $\text{Gal}(H/H')$. Thus, K is p -rational if and only if B is trivial.

Corollary 4.1.6 then follows immediately from the following intrinsic description of B . Suppose that \mathfrak{a} is a fraction ideal of K and that the class $a = cl(\mathfrak{a})$ is in A . Thus $\mathfrak{a}^{p^t} = \alpha \mathcal{O}_K$ for some $t \geq 0$ and some $\alpha \in K^\times$. We will say that \mathfrak{a} is a “singular ideal” and that a is a “singular class” if the following condition is satisfied: *A generator α for \mathfrak{a}^{p^t} is a p^t -th power in K_v^\times for all v dividing p .* It is easy to verify that this definition depends only on the ideal class a and not on the choice of \mathfrak{a}, α , or t . The set of singular classes in A is obviously a subgroup of A . This subgroup is precisely B . It is not difficult to prove this by using the description of Γ_K^{ab} given by class field theory. The ray class formulation is the most convenient. We omit the details. ◇

4.2. Compositums of quadratic fields. Suppose now that $\Omega = \text{Gal}(K/\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z})^t$ for some $t \geq 2$. If $\chi \in \widehat{\Omega}$, and $\chi \neq \chi_0$, then $\ker(\chi)$ is a subgroup of Ω of index 2. We let F_χ denote the corresponding quadratic extension of \mathbf{Q} . All the quadratic subfields of K are of the form F_χ for some $\chi \neq \chi_0$. There are $2^t - 1$ such subfields. Proposition 3.3.1 shows that K is p -rational if and only if all of the quadratic field F_χ 's are p -rational. It seems reasonable to make the following conjecture, although our numerical evidence is not very strong.

Conjecture 4.2.1. *For any odd prime p and for any t , there exists a p -rational field K such that $\text{Gal}(K/\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z})^t$.*

We can merely give a few examples. For $p = 3$, we use corollary 4.1.2 to check 3-rationality. For $p = 5$, we use corollary 4.1.4 for the real quadratic subfields of K . For the imaginary quadratic subfields, we can just check either that the class number is not divisible by 5 or we can use corollary 4.1.6 if the class number is divisible by 5.

$$p = 3, t = 5 : \quad K = \mathbf{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{5}, \sqrt{11}, \sqrt{97})$$

$$p = 3, t = 6 : \quad K = \mathbf{Q}(\sqrt{-1}, \sqrt{13}, \sqrt{145}, \sqrt{209}, \sqrt{269}, \sqrt{373})$$

$$p = 5, t = 5 : \quad K = \mathbf{Q}(\sqrt{-1}, \sqrt{6}, \sqrt{11}, \sqrt{14}, \sqrt{59})$$

The example for $p = 3$ and $t = 5$ was found by Sourav Sen Gupta. The example for $p = 3$ and $t = 6$ was found by Robert Bradshaw. In both cases, a number of examples were found, although only a very small proportion of the trial set. The example for $p = 5$ was found by the author. The verification requires using the criterion in corollary 4.1.6 for just one of the imaginary quadratic subfields of K , namely $F = \mathbf{Q}(\sqrt{-11 \cdot 59})$.

4.3. The field $K = \mathbf{Q}(\mu_p)$. Under the assumption that p is a regular prime, Shafarevich proved that Γ_K is a free pro- p group if $K = \mathbf{Q}(\mu_p)$. One finds this on page 139 in [Sha], an illustration of general results in that paper about generators and relations for certain Galois groups. Using the results about p -rationality cited in section 3, we can give a rather short argument.

Proposition 4.3.1. *Let $K = \mathbf{Q}(\mu_p)$. Suppose that p is a regular prime. Then K is a p -rational field.*

Proof. We are assuming that the class group of K has no elements of order p . Let $\varepsilon_1, \dots, \varepsilon_r$ be a fundamental set of units for K , where $r = r_2(K) - 1$. Let ζ_p be a generator for μ_p . Then a straightforward Kummer theory argument shows that

$$L = K \left(\sqrt[p]{p}, \sqrt[p]{\zeta_p}, \sqrt[p]{\eta_1}, \dots, \sqrt[p]{\eta_r} \right) .$$

where L is the fixed field for $\Phi(\Gamma_K)$. Consequently, one sees that

$$\dim_{\mathbf{F}_p}(\text{Gal}(L/K)) = r + 2 = r_2(K) + 1 .$$

It follows that the inequalities (3) are equalities. Therefore K is indeed a p -rational field. ■

4.4. The field $K = \mathbf{Q}(\mu_5)$ and $p \neq 5$. It is known that the class number of K is 1. Also, μ_p is not contained in the completion of K at the primes lying above p . It follows

that $(\Gamma_K^{ab})^{\epsilon_\chi}$ is torsion-free when χ is a faithful, irreducible representation of $\Omega = \text{Gal}(K/\mathbf{Q})$. Such a representation χ is odd. If $p \equiv 1 \pmod{4}$, then there are two such χ 's, both 1-dimensional over \mathbf{Q}_p , but if $p \equiv 3 \pmod{4}$, then there is just one such χ , a 2-dimensional representation over \mathbf{Q}_p . One then sees from the proof of proposition 3.3.1 that $K = \mathbf{Q}(\mu_5)$ will be p -rational if and only if $(\Gamma_K^{ab})^{\epsilon_\chi}$ is torsion-free when χ is the character of Ω of order 2, which in turn means that the field $\mathbf{Q}(\sqrt{5})$ is p -rational. Corollary 4.1.5 gives a useful criterion involving Fibonacci numbers. Thus, we see that $K = \mathbf{Q}(\mu_5)$ is p -rational if and only if $F_q \not\equiv 1 \pmod{p^2}$, where $q = p$ if p is a quadratic residue modulo 5, $q = p^2$ if p is a quadratic nonresidue modulo 5.

We have searched for primes p for which K fails to be p -rational. The criterion just stated suggests that such p 's are quite rare, but should exist. We haven't found any. In particular, K turns out to be p -rational for all $p < 10,000$ and, if p is a quadratic residue, even for all $p < 8,000,000$. We did this verification using Sage. In the latter case, R. Pollack verified that K is p -rational for the much larger range of primes $p < 3 \times 10^9$. As we will explain in section 6, if p is a prime such that $4|(p-1)$, and if K is p -rational, then one can construct 3-dimensional Galois representations of $\text{Gal}(M_K/\mathbf{Q})$ over \mathbf{Q}_p with open image.

5 A Sylow pro- p subgroup of $SL_n(\mathbf{Z}_p)$.

We assume that $n \geq 2$ and that $p \geq 3$ throughout. We will first describe our notation for various groups. If R is any commutative ring with identity, then $T_n(R)$ denotes the group of diagonal matrices in $GL_n(R)$, $U_n(R)$ denotes the group of upper triangular matrices in $GL_n(R)$ with diagonal entries equal to 1_R , and $B_n(R) = T_n(R)U_n(R)$ is the group of invertible upper triangular matrices. The $n \times n$ identity and zero matrices will be denoted by I_n and O_n for any ring R . We will also use the notation E_{ij} to denote the matrix whose entries are all zeros except for a 1_R as the entry on the i -th row and j -th column. The ring, or the additive group, of $n \times n$ matrices over R will be denoted by $M_n(R)$. The R -submodule consisting of matrices with trace equal to 0_R will be denoted by $M_n^{(0)}(R)$. Of course, $SL_n(R)$ denotes the kernel of the determinant map $\det : GL_n(R) \rightarrow R^\times$.

Suppose that $R = \mathbf{Z}_p$. If $r \geq 1$, then the congruence subgroup $I_n + p^r M_n(\mathbf{Z}_p)$ of $GL_n(\mathbf{Z}_p)$ will be denoted by $C_n(p^r)$. Thus, $C_n(p^r)$ is a normal subgroup of $GL_n(\mathbf{Z}_p)$ and the corresponding quotient group is isomorphic to $GL_n(\mathbf{Z}/p^r\mathbf{Z})$. The torsion subgroup of $T_n(\mathbf{Z}_p)$ will be denoted by Θ_n . It is the subgroup of diagonal matrices whose diagonal entries are $(p-1)$ -st roots of unity. For $1 \leq i \leq n$ and $\tau \in \Theta_n$, we let $\theta_i(\tau)$ denote the i -th diagonal entry of τ . Thus, $\theta_i : \Theta_n \rightarrow \mathbf{Z}_p^\times$ is a character of Θ_n of order $p-1$. The reduction map $GL_n(\mathbf{Z}_p) \rightarrow GL_n(\mathbf{F}_p)$ induces a surjective homomorphism $T_n(\mathbf{Z}_p) \rightarrow T_n(\mathbf{F}_p)$. The restriction

to Θ_n defines an isomorphism $\Theta_n \rightarrow T_n(\mathbf{F}_p)$. We identify those two groups and regard the characters θ_i as characters of $T_n(\mathbf{F}_p)$ or of Θ_n , with values in \mathbf{Z}_p^\times or in \mathbf{F}_p^\times , depending on the context.

Let $\mathfrak{Z} = \mathbf{Z}_p^n$. We let $\{\mathfrak{z}_1, \dots, \mathfrak{z}_n\}$ be the standard \mathbf{Z}_p -module basis for \mathfrak{Z} . Thus, the entries of \mathfrak{z}_i are all 0's, except for the i -th entry which is 1. Let $GL_n(\mathbf{Z}_p)$ act on \mathfrak{Z} by matrix multiplication, regarding the elements of \mathfrak{Z} as column matrices. The Frattini quotient $\tilde{\mathfrak{Z}} = \mathfrak{Z}/p\mathfrak{Z}$ is isomorphic to \mathbf{F}_p^n . The induced action of $GL_n(\mathbf{Z}_p)$ on $\tilde{\mathfrak{Z}}$ factors through the quotient group $GL_n(\mathbf{F}_p)$ and is again just matrix multiplication. Since $C_n(p)$ is a normal pro- p -subgroup of $GL_n(\mathbf{Z}_p)$, a Sylow pro- p subgroup of $GL_n(\mathbf{Z}_p)$ is determined by specifying a Sylow p -subgroup of $GL_n(\mathbf{F}_p)$. We can specify such a subgroup by choosing an ascending sequence of \mathbf{F}_p -subspaces $\tilde{\mathfrak{Z}}_i$ for $0 \leq i \leq n$, where $\tilde{\mathfrak{Z}}_i$ has dimension i . The set of elements of $GL_n(\mathbf{F}_p)$ which leave those subspaces fixed and which act trivially on $\tilde{\mathfrak{Z}}_i/\tilde{\mathfrak{Z}}_{i-1}$ for $i \geq 1$ is a Sylow p -subgroup. We simply choose $\tilde{\mathfrak{Z}}_i$ to be the subspace generated by $\{\tilde{\mathfrak{z}}_1, \dots, \tilde{\mathfrak{z}}_i\}$ for $i \geq 1$. The Sylow p -subgroup thus specified is $U_n(\mathbf{F}_p)$, as defined above. The corresponding Sylow pro- p -subgroup of $GL_n(\mathbf{Z}_p)$ will be denoted by $S_n(\mathbf{Z}_p)$. We have $S_n(\mathbf{Z}_p) = C_n(p)U_n(\mathbf{Z}_p)$ by definition.

5.1. Special elements of $SL_n(\mathbf{Z}_p)$. The E_{ij} 's satisfy the following simple multiplication law: $E_{ab}E_{cd} = \delta_{bc}E_{ad}$, where δ_{bc} is 1 if $b = c$ and is 0 otherwise. It follows that $E_{ij}^2 = O_n$ if $i \neq j$. Therefore, if $i \neq j$ and if a is a positive integer, then

$$(5) \quad (I_n + E_{ij})^a = I_n + aE_{ij} \quad .$$

This shows that $(I_n + E_{ij})^a \rightarrow I_n$ as $a \rightarrow 0$ p -adically. Hence $\overline{\langle I_n + E_{ij} \rangle}$ is a pro- p subgroup of $SL_n(\mathbf{Z}_p)$ and is isomorphic to \mathbf{Z}_p . Furthermore, (5) holds for all $a \in \mathbf{Z}_p$. If $j > i$, then $\overline{\langle I_n + E_{ij} \rangle} \subset U_n(\mathbf{Z}_p)$.

Suppose that $D \in T_n(\mathbf{Z}_p)$. Thus, $D = \sum_{i=1}^n d_i E_{ii}$, where $d_i \in \mathbf{Z}_p^\times$ for $1 \leq i \leq n$. Of course, $D^{-1} = \sum_{i=1}^n d_i^{-1} E_{ii}$. The following relationship follows immediately from the multiplication law and will be quite useful:

$$(6) \quad D(I_n + E_{ij})D^{-1} = I_n + d_i d_j^{-1} E_{ij} = (I_n + E_{ij})^{d_i d_j^{-1}}$$

for any i and j with $i \neq j$. In particular, this applies when $D \in \Theta_n$ in which case we have $d_i d_j^{-1} = (\theta_i \theta_j^{-1})(D)$. If we take $\Omega = \Theta_n$, then $\overline{\langle I_n + E_{ij} \rangle}$ is an Ω -group in the sense of section 2. More precisely, $I_n + E_{ij}$ is a χ -element, where χ is the \mathbf{Z}_p^\times -valued character $\theta_i \theta_j^{-1}$ of Θ_n .

5.2. The structure of $U_n(\mathbf{F}_p)$. It is obvious that $U_n(\mathbf{F}_p)$ is a p -group. Every element of $U_n(\mathbf{F}_p)$ has the form $I_n + A$, where A can be written in the form $A = \sum_{j>i} a_{ij} E_{ij}$. Here, the

a_{ij} 's are in \mathbf{F}_p . The following properties of $U_n(\mathbf{F}_p)$ are well-known. The Frattini subgroup $\Phi(U_n(\mathbf{F}_p))$ consists of elements $I + A$ where $a_{ij} = 0$ when $j - i = 1$. Equivalently, $\Phi(U_n(\mathbf{F}_p))$ consists of the invertible matrices which leave the subspaces $\tilde{\mathfrak{Z}}_i$ fixed and which act trivially on the 2-dimensional subquotients $\tilde{\mathfrak{Z}}_i/\tilde{\mathfrak{Z}}_{i-2}$ for $2 \leq i \leq n$. It follows that

$$U_n(\mathbf{F}_p)/\Phi(U_n(\mathbf{F}_p)) \cong \mathbf{F}_p^{n-1}$$

as a group. With the above notation, the isomorphism is defined by sending $I + A$ to $(a_{12}, \dots, a_{(n-1)n})$. It is then clear that the set

$$(7) \quad \{ I_n + E_{ij} \mid j = i + 1, \text{ where } 1 \leq i \leq n - 1 \}$$

is a minimal set of generators for $U_n(\mathbf{F}_p)$. Its cardinality is $n - 1$.

Alternatively, one can verify that (7) generates $U_n(\mathbf{F}_p)$ by the following induction argument. It is clear for $n = 2$ and, if $n \geq 3$, one can identify $U_{n-1}(\mathbf{F}_p)$ with the subgroup of $U_n(\mathbf{F}_p)$ consisting of elements which fix $\tilde{\mathfrak{Z}}_n$. Assume that this subgroup $U_{n-1}(\mathbf{F}_p)$ is generated by the first $n - 2$ elements in (7). Now the kernel of the restriction map r defined by $r(A) = A|_{\tilde{\mathfrak{Z}}_{n-1}}$ is the subgroup generated by $\{I_n + E_{jn} \mid 1 \leq j \leq n - 1\}$, which is an elementary abelian p -group. One sees that $U_n(\mathbf{F}_p)$ is the semidirect product of $U_{n-1}(\mathbf{F}_p)$ and $\ker(r)$. Furthermore, when $U_{n-1}(\mathbf{F}_p)$ acts on $\ker(r)$ by conjugation, one checks easily that the orbit of $I_n + E_{(n-1)n}$ generates $\ker(r)$. Thus, it would follow that (7) is a generating set for $U_n(\mathbf{F}_p)$.

5.3. The action of $U_n(\mathbf{F}_p)$ on $M_n(\mathbf{F}_p)$. We let $U_n(\mathbf{F}_p)$ act on $M_n(\mathbf{F}_p)$ by conjugation. That is, if $u \in U_n(\mathbf{F}_p)$ and $A \in M_n(\mathbf{F}_p)$, then u acts by sending A to $u(A) = uAu^{-1}$. Thus, $M_n(\mathbf{F}_p)$ becomes an \mathbf{F}_p -representation space for $U_n(\mathbf{F}_p)$ of degree n^2 . Thus, $M_n(\mathbf{F}_p)$ can be regarded as a module over the group ring $\mathbf{F}_p[U_n(\mathbf{F}_p)]$. The following result is crucial for this paper.

Proposition 5.3.1. *The $\mathbf{F}_p[U_n(\mathbf{F}_p)]$ -module $M_n^{(0)}(\mathbf{F}_p)$ is cyclic. It is generated by E_{n1} .*

Proof. For brevity, let $U = U_n(\mathbf{F}_p)$. Consider the \mathbf{F}_p -bilinear pairing

$$\langle \cdot, \cdot \rangle : M_n(\mathbf{F}_p) \times M_n(\mathbf{F}_p) \longrightarrow \mathbf{F}_p$$

defined as follows: $\langle A, B \rangle = \text{Tr}(AB)$ for all $A, B \in M_n(\mathbf{F}_p)$. It is clear that this pairing is non-degenerate. We also have $\langle u(A), u(B) \rangle = \langle A, B \rangle$ for all $u \in U$ and $A, B \in M_n(\mathbf{F}_p)$. Consequently, the \mathbf{F}_p -representation space $M_n(\mathbf{F}_p)$ for U is self-dual.

Suppose that W is an \mathbf{F}_p -subspace of $M_n(\mathbf{F}_p)$. We let W^\perp denote the orthogonal complement of W with respect to the pairing $\langle \cdot, \cdot \rangle$. If W is invariant under the action of U , then so is W^\perp . Moreover, the above pairing induces a non-degenerate \mathbf{F}_p -bilinear pairing $W^\perp \times (M_n(\mathbf{F}_p)/W) \rightarrow \mathbf{F}_p$ which is also equivariant for the action of U . In particular, let $W = \mathbf{F}_p I_n$. Then $W^\perp = M_n^{(0)}$ and we obtain a nondegenerate, U -equivariant pairing

$$M_n^{(0)}(\mathbf{F}_p) \times (M_n(\mathbf{F}_p)/\mathbf{F}_p I_n) \longrightarrow \mathbf{F}_p .$$

This means that the two \mathbf{F}_p -representation spaces $M_n^{(0)}(\mathbf{F}_p)$ and $M_n(\mathbf{F}_p)/\mathbf{F}_p I_n$ for U are dual to each other.

The ring $\mathbf{F}_p[U]$ is local. Its maximal ideal is the augmentation ideal \mathfrak{m} . That ideal is generated by the elements $u - I_n$, where u varies over U . To prove that a nontrivial $\mathbf{F}_p[U]$ -module M is cyclic, one must show that $M/\mathfrak{m}M$ is 1-dimensional over \mathbf{F}_p . Note that $M/\mathfrak{m}M$ is the maximal quotient M_U of M on which U acts trivially. If $N = \text{Hom}_{\mathbf{F}_p}(M, \mathbf{F}_p)$, then M_U is dual to N^U , the maximal submodule of N on which U acts trivially. Therefore, the following lemma implies proposition 5.3.1.

Lemma 5.3.2. *For any $n \geq 2$ and any odd prime p , we have*

$$\left(M_n(\mathbf{F}_p)/\mathbf{F}_p I_n \right)^U = (\mathbf{F}_p I_n + \mathbf{F}_p E_{1n})/\mathbf{F}_p I_n ,$$

an \mathbf{F}_p -vector space of dimension 1.

Proof. The group U acts on the \mathbf{F}_p -vector space $\tilde{\mathfrak{Z}}$. One sees easily that the only subspaces of $\tilde{\mathfrak{Z}}$ which are invariant under the action of U are the $\tilde{\mathfrak{Z}}_i$'s, where $0 \leq i \leq n$. Note that $(\tilde{\mathfrak{Z}}/\tilde{\mathfrak{Z}}_i)^U = \tilde{\mathfrak{Z}}_{i+1}/\tilde{\mathfrak{Z}}_i$ for $0 \leq i \leq n-1$. It will also be useful to note that the action of U on the unique 2-dimensional quotient $\tilde{\mathfrak{Z}}/\tilde{\mathfrak{Z}}_{n-2}$ is nontrivial and that if $n \geq 3$ and $2 \leq i < n$, then $\tilde{\mathfrak{Z}}_i/\tilde{\mathfrak{Z}}_{i-2}$ is *not* isomorphic to $\tilde{\mathfrak{Z}}/\tilde{\mathfrak{Z}}_{n-2}$ as an $\mathbf{F}_p[U]$ -module. This is clear since the action of $I_n + E_{(n-1)n}$ is trivial on the first module and nontrivial on the second.

We first show that $M_n(\mathbf{F}_p)^U = \mathbf{F}_p I_n + \mathbf{F}_p E_{1n}$. The inclusion in one direction is obvious. For the other direction, suppose that $A \in M_n(\mathbf{F}_p)^U$. This means that $uA = Au$ for all $u \in U$. Since $\tilde{\mathfrak{Z}}_1 = \tilde{\mathfrak{Z}}^U$, one sees that $A\tilde{\mathfrak{Z}}_1 \subseteq \tilde{\mathfrak{Z}}_1$. A simple induction argument shows that $A\tilde{\mathfrak{Z}}_i \subseteq \tilde{\mathfrak{Z}}_i$ for all i . Thus, A is upper triangular. Now $A\tilde{\mathfrak{Z}}_1 = a\tilde{\mathfrak{Z}}_1$ for some $a \in \mathbf{F}_p$. Let $B = A - aI_n$, which is also in $M_n(\mathbf{F}_p)^U$ and is a singular matrix. It follows that $B\tilde{\mathfrak{Z}}$ is a U -invariant subspace of $\tilde{\mathfrak{Z}}$ and hence that $B\tilde{\mathfrak{Z}} = \tilde{\mathfrak{Z}}_i$ for some $i \leq n-1$. In fact, we must have $i \leq 1$. For otherwise, multiplication by B would define an isomorphism from $\tilde{\mathfrak{Z}}/\tilde{\mathfrak{Z}}_{n-2}$ onto $\tilde{\mathfrak{Z}}_i/\tilde{\mathfrak{Z}}_{i-2}$, and this is not possible. Therefore, $B\tilde{\mathfrak{Z}}_i = 0$ for all $i \leq n-1$ and $B\tilde{\mathfrak{Z}}_n = b\tilde{\mathfrak{Z}}_1$

for some $b \in \mathbf{F}_p$. Consequently, $B = bE_{1n}$. Hence, we indeed have $A = aI_n + bE_{1n}$, where $a, b \in \mathbf{F}_p$.

Suppose that $p \nmid n$. Then $M_n(\mathbf{F}_p)$ is a direct sum $\mathbf{F}_p I_n + M_n^{(0)}(\mathbf{F}_p)$ as an $\mathbf{F}_p[U]$ -module. We therefore have an isomorphism $M_n(\mathbf{F}_p)/\mathbf{F}_p I_n \cong M_n^{(0)}(\mathbf{F}_p)$. We also have $M_n^{(0)}(\mathbf{F}_p)^U = \mathbf{F}_p E_{1n}$. Thus, the stated conclusion is now clear if $p \nmid n$. Note also that $M_n^{(0)}(\mathbf{F}_p)$ is a self-dual representation space for U in this case.

If $p \mid n$, then we can use the following alternative argument which just requires that $n \geq 3$. Suppose that $A \in M_n(\mathbf{F}_p)$ and that $uAu^{-1} - A \in \mathbf{F}_p I_n$ for all $u \in U$. For any pair (s, t) such that $1 \leq s < t \leq n$, let $u = I_n + E_{st}$. Then $u^{-1} = I_n - E_{st}$ and we have

$$uAu^{-1} - A = E_{st}A - AE_{st} - E_{st}AE_{st} ,$$

which is a matrix whose nonzero entries can only be in row s or in column t . Since $n \geq 3$, this matrix can be equal to cI_n , where $c \in \mathbf{F}_p$, only if $c = 0$. Thus, $uAu^{-1} = A$ for all u 's of the above form. Since U is generated by the set (7), it follows that $A \in M_n(\mathbf{F}_p)^U$. The conclusion then follows from the first step in the proof.

An element $A \in M_n^{(0)}(\mathbf{F}_p)$ will be a generator of $M_n^{(0)}(\mathbf{F}_p)$ as an $\mathbf{F}_p[U]$ -module if and only if A has a nontrivial image in $M_n^{(0)}(\mathbf{F}_p)_U$. This means that A is not orthogonal to E_{1n} . One such element is $A = E_{n1}$. We have $\langle E_{n1}, E_{1n} \rangle = 1$. \blacksquare

5.4. Generators for a Sylow pro- p subgroup of $SL_n(\mathbf{Z}_p)$. We let $C_n^{(0)}(p^r)$ and $S_n^{(0)}(\mathbf{Z}_p)$ denote the intersections $C_n(p^r) \cap SL_n(\mathbf{Z}_p)$ and $S_n(\mathbf{Z}_p) \cap SL_n(\mathbf{Z}_p)$, respectively. The Sylow pro- p -subgroup of $SL_n(\mathbf{Z}_p)$ is $S_n^{(0)}(\mathbf{Z}_p)$, which can also be described as $C_n^{(0)}(p)U_n(\mathbf{Z}_p)$. Thus, $S_n^{(0)}(\mathbf{Z}_p)$ has a descending sequence of normal subgroups $C_n^{(0)}(p^r)$ for $r \geq 1$, $S_n^{(0)}(\mathbf{Z}_p)/C_n^{(0)}(p)$ is isomorphic to $U_n(\mathbf{F}_p)$, and $C_n^{(0)}(p^r)/C_n^{(0)}(p^{r+1})$ is isomorphic to the additive group of $M_n^{(0)}(\mathbf{F}_p)$ for all $r \geq 1$. The latter isomorphisms are defined by the maps defined by sending the coset represented by a matrix of the form $I_n + p^r A$, where $A \in M_n(\mathbf{Z}_p)$, to the image \bar{A} of A in $M_n(\mathbf{F}_p)$. This defines an isomorphism

$$C_n(p^r)/C_n(p^{r+1}) \longrightarrow M_n(\mathbf{F}_p)$$

which is equivariant for the natural actions of $U_n(\mathbf{F}_p)$ on those two groups (defined by conjugation). This isomorphism is easily seen to send the subgroup represented by matrices of determinant 1 onto $M_n^{(0)}(\mathbf{F}_p)$. Proposition 5.3.1 then implies that $C_n^{(0)}(p^r)/C_n^{(0)}(p^{r+1})$ is generated as a group by the $U_n(\mathbf{F}_p)$ -orbit of the element which is represented by the matrix $I_n + p^r E_{n1}$. Note that $I_n + p^r E_{n1}$ is a power of $I_n + pE_{n1}$ for all $r \geq 1$.

The above remarks and a straightforward induction argument give the following result.

Proposition 5.4.1. *The Sylow pro- p subgroup $S_n^{(0)}(\mathbf{Z}_p)$ of $SL_n(\mathbf{Z}_p)$ can be generated topologically by*

$$(8) \quad \{ I_n + E_{ij} \mid j = i + 1, \text{ where } 1 \leq i \leq n - 1 \} \cup \{ I_n + pE_{n1} \} .$$

This is a minimal generating set for $S_n^{(0)}(\mathbf{Z}_p)$. It has cardinality n .

Alternatively, one can verify this by using the fact that the Frattini subgroup of $C_n(p)$ is $C_n(p^2)$, proposition 5.3.1, and the **BBT**. The set (8) is a minimal topological generating set for $S_n^{(0)}(\mathbf{Z}_p)$. To see this, note that the first set in the union is contained in $U_n(\mathbf{Z}_p)$. The images of those $n - 1$ elements in the Frattini quotient of $S_n^{(0)}(\mathbf{Z}_p)$ are linearly independent over \mathbf{F}_p . They don't generate $S_n^{(0)}(\mathbf{Z}_p)$ and hence cannot be a basis for the Frattini quotient of that group. Therefore, at least n elements are needed to generate $S_n^{(0)}(\mathbf{Z}_p)$ topologically. We also remark that one obtains a minimal topological generating set for the Sylow pro- p subgroup $S_n(\mathbf{Z}_p)$ of $GL_n(\mathbf{Z}_p)$ by just including any additional matrix A such that $\det(A) = 1 + p$. For example, one can take $A = I_n + pE_{nn}$.

5.5. The action of Θ_n . If we take $\Omega = \Theta_n$, then the elements in (8) are Ω -elements. This follows from (6). The corresponding characters (in the listed order) are: $\theta_1\theta_2^{-1}, \dots, \theta_{n-1}\theta_n^{-1}$, and $\theta_n\theta_1^{-1}$. These characters are all distinct. Their product is the trivial character of Θ_n . If we choose a diagonal matrix A with determinant $1 + p$, then such an A will also be an Ω -element. The corresponding character is the trivial character of Θ_n .

More generally, suppose that Ω is a group satisfying assumption **A** stated in section 2. Suppose that we fix a homomorphism $\omega : \Omega \rightarrow \Theta_n$. Such an ω is determined by specifying the elements $\omega_i = \theta_i \circ \omega$ of $\widehat{\Omega}$ for $1 \leq i \leq n$. We can then regard $S_n^{(0)}(\mathbf{Z}_p)$ as an Ω -group. The set (8) consists of Ω -elements and the corresponding characters are $\omega_1\omega_2^{-1}, \dots, \omega_{n-1}\omega_n^{-1}$, and $\omega_n\omega_1^{-1}$. Of course, they are not necessarily distinct. Their product is the trivial character χ_0 of Ω . This observation determines the Ω -type of $S_n^{(0)}(\mathbf{Z}_p)$. It is simply the direct sum of the above listed characters. The Ω -type of $S_n(\mathbf{Z}_p)$ is then obtained by including an additional χ_0 in the direct sum.

We now prove a result which is useful for certain applications, although we will not need it in this paper. Suppose that (s, t) is a pair of integers such that $1 \leq s, t \leq n$. Let Ω and ω be as in the previous paragraph. We will say that (s, t) is (Ω, ω) -distinguished if the following statement is satisfied:

$$\text{If } 1 \leq i, j \leq n \text{ and } \omega_i\omega_j^{-1} = \omega_s\omega_t^{-1}, \text{ then } (i, j) = (s, t).$$

In particular, since $n \geq 2$, this statement implies that $s \neq t$. The following proposition will be useful in [Gr2], but only for the case where $n = 2$. In that case, the pair $(1, 2)$ is (Ω, ω) -distinguished if and only if the order of the character $\omega_1\omega_2^{-1}$ is not 1 or 2.

Proposition 5.5.1. *Suppose that $p - 1 > n$ and that (s, t) is (Ω, ω) -distinguished. Suppose that $A \in GL_n(\mathbf{Z}_p)$ and that the image of A in $GL_n(\mathbf{F}_p)$ is of p -power order. Suppose that A is an Ω -element and that the corresponding character is $\omega_s\omega_t^{-1}$. Then $A = (I_n + E_{st})^a$ for some $a \in \mathbf{Z}_p$.*

Proof. First note that $A^{p^k} \in C_n(p)$ for some $k \geq 0$. Thus, $\overline{\langle A \rangle}$ is a pro- p subgroup of $GL_n(\mathbf{Z}_p)$. If $r \geq 1$, then one can define a function $\log : C_n(p^r) \rightarrow M_n(\mathbf{Z}_p)$ by the usual power series expansion. We take r sufficiently large so that the image of the above map is contained in the domain where the power series expansion for the exponential function converges and gives a left inverse for \log , which we denote by \exp . Then \log will be injective on $C_n(p^r)$. Another property is that if $B \in C_n(p^r)$ and $b \in \mathbf{Z}_p$, then $\log(B^b) = b \cdot \log(B)$. This is a formal property of the power series defining \log . In addition, it is clear that if $T \in GL_n(\mathbf{Z}_p)$ and $B \in C_n(p^r)$, then $\log(TBT^{-1}) = T\log(B)T^{-1}$.

Suppose that A satisfies the assumptions in the proposition. Let $\chi = \omega_s\omega_t^{-1}$, a nontrivial character of Ω . Then A^{p^m} is in $C_n(p^r)$ for some $m \geq 1$ and is a χ -element. Now we can also use ω to make the additive group of $M_n(\mathbf{Z}_p)$ into an Ω -group. An element $\alpha \in \Omega$ acts as conjugation by the matrix $\omega(\alpha)$. It follows that $\log(A^{p^m})$ is a χ -element of $M_n(\mathbf{Z}_p)$. The assumption that (s, t) is (Ω, ω) -distinguished implies that $\log(A^{p^m}) = kE_{st}$ for some $k \in \mathbf{Z}_p$. Since $s \neq t$, we have $E_{st}^2 = O_n$. As a consequence of these remarks, together with (5), we have

$$A^{p^m} = \exp(kE_{st}) = I_n + kE_{st} = (I_n + E_{st})^k$$

for some $k \in \mathbf{Z}_p$. In particular, A^{p^m} is a unipotent matrix. Thus, the eigenvalues of A are p -power roots of unity. Since $n < p - 1 = [\mathbf{Q}_p(\mu_p) : \mathbf{Q}_p]$, it follows that A itself is unipotent.

If $k = 0$, then one sees easily that $A = I_n$ and one can take $a = 0$. We now assume that $k \neq 0$. Consider A and E_{st} as endomorphisms of the vector space $\mathcal{V} = \mathfrak{z} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Note that $A^{p^m} - I_n = (A - I_n)B$, where B is invertible in $M_n(\mathbf{Q}_p)$. Thus, $A - I_n$ and $A^{p^m} - I_n$ have the same kernel and the same image as endomorphisms of \mathcal{V} , which are also the same as the kernel and the image of E_{st} , respectively. The common kernel has codimension 1 and is generated by the \mathfrak{z}_i 's with $i \neq t$. The common image is $\mathbf{Q}_p\mathfrak{z}_s$ and so $(A - I_n)\mathfrak{z}_t = a\mathfrak{z}_s$ for some $a \in \mathbf{Q}_p$. Clearly, $a \in \mathbf{Z}_p$. It follows that $A - I_n = aE_{st}$ and the stated conclusion then follows by using (5). ■

5.6. The Ω -type of the pro- p group $C_n(p)$. We assume that Ω has order prime to p and that we are given a homomorphism $\bar{\omega} : \Omega \rightarrow GL_n(\mathbf{F}_p)$. Then we know that $\bar{\omega}$ can be

lifted to a homomorphism $\omega : \Omega \rightarrow GL_n(\mathbf{Z}_p)$. If $\alpha \in \Omega$, then we can let α act on $C_n(p)$ as conjugation by the matrix $\omega(\alpha)$. Thus, $C_n(p)$ becomes an Ω -group. The Frattini quotient is

$$\widetilde{C_n(p)} = C_n(p)/C_n(p^2) \cong M_n(\mathbf{F}_p) \quad .$$

Thus, the minimal cardinality of a topological generating set for $C_n(p)$ is n^2 . The Ω -type of $C_n(p)$ is determined by $\bar{\omega}$ and is defined by letting $\alpha \in \Omega$ act on $M_n(\mathbf{F}_p)$ as conjugation by the matrix $\bar{\omega}(\alpha)$. This representation of Ω is isomorphic to the tensor product (over \mathbf{F}_p) of $\bar{\omega}$ and the contragredient of $\bar{\omega}$. If we let $\tilde{\omega}$ denote the contragredient of ω , then the Ω -type of $C_n(p)$ is obtained from $\omega \otimes_{\mathbf{Z}_p} \tilde{\omega}$ by reduction modulo p . The resulting representation of Ω over \mathbf{F}_p is the so-called adjoint representation (corresponding to $\bar{\omega}$) and will be denoted by $ad(\bar{\omega})$.

6 The construction.

We assume that K/\mathbf{Q} is a finite abelian extension, that p is an odd prime, and that $\Omega = \text{Gal}(K/\mathbf{Q})$ has exponent dividing $p - 1$. As in section 3, we let $M = M_K$ denote the maximal pro- p extension of K which is unramified outside of the set of primes above p . Let $\Gamma = \Gamma_K = \text{Gal}(M/K)$. The action of $G_{\mathbf{Q}}$ on μ_{p^∞} defines a continuous homomorphism χ_{cyc} from $G_{\mathbf{Q}}$ to $GL_1(\mathbf{Z}_p) = \mathbf{Z}_p^\times$. It is surjective. Now $1 + p\mathbf{Z}_p$ is a direct factor in \mathbf{Z}_p^\times . Composing χ_{cyc} with the projection map defines a surjective homomorphism $\kappa : G_{\mathbf{Q}} \rightarrow 1 + p\mathbf{Z}_p$. One sees easily that κ factors through $\text{Gal}(M/\mathbf{Q})$.

6.1. The basic proposition. Our construction of continuous representations into $GL_n(\mathbf{Z}_p)$ with open image is based on the following result.

Proposition 6.1.1. *Assume that K is p -rational and that $\Omega = \text{Gal}(K/\mathbf{Q})$ has exponent dividing $p - 1$. Assume also that one can find distinct characters χ_1, \dots, χ_n in $\widehat{\Omega}_{odd} \cup \{\chi_0\}$ such that their product is χ_0 . Then there exists a continuous homomorphism*

$$\rho_0 : \text{Gal}(M/\mathbf{Q}) \longrightarrow GL_n(\mathbf{Z}_p)$$

such that $\rho_0(\Gamma) = S_n^{(0)}(\mathbf{Z}_p)$. Furthermore, $\rho = \rho_0 \otimes \kappa$ is a continuous homomorphism from $\text{Gal}(M/\mathbf{Q})$ to $GL_n(\mathbf{Z}_p)$ with open image.

Proof. We may as well assume that $n \geq 2$. The result is trivial for $n = 1$. Thus, $\widehat{\Omega}_{odd}$ is nonempty and K is totally complex. If $\omega : \Omega \rightarrow \Theta_n$ is a homomorphism, then we let $\omega_i = \theta_i \circ \omega$ for $1 \leq i \leq n$. The ω_i 's are in $\widehat{\Omega}$. We specify ω by choosing the ω_i 's so that

$$\omega_1 \omega_2^{-1} = \chi_1, \quad \dots, \quad \omega_{n-1} \omega_n^{-1} = \chi_{n-1}, \quad \text{and} \quad \omega_n \omega_1^{-1} = \chi_n \quad .$$

If we choose $\omega_1 \in \widehat{\Omega}$ arbitrarily, and choose χ_1, \dots, χ_n as stated in the proposition, then the first $n - 1$ of these equations will determine a certain ω . The assumption about the product of the χ_i 's makes the n -th equation satisfied too.

Note that Θ_n normalizes $S_n^{(0)}(\mathbf{Z}_p)$. If $\alpha \in \Omega$, then we can let α act on $S_n^{(0)}(\mathbf{Z}_p)$ as conjugation by $\omega(\alpha)$. Hence, $S_n^{(0)}(\mathbf{Z}_p)$ becomes an Ω -group. Furthermore, there is a homomorphism from the corresponding semidirect product $S_n^{(0)}(\mathbf{Z}_p) \rtimes \Omega$ to $GL_n(\mathbf{Z}_p)$. It is defined by making it the identity map on $S_n^{(0)}(\mathbf{Z}_p)$ and the map ω on Ω .

As pointed out in section 5.5, the generators of $S_n^{(0)}(\mathbf{Z}_p)$ listed in proposition 5.4.1 are Ω -elements and the corresponding characters are χ_1, \dots, χ_n , respectively. We will denote them by s_1, \dots, s_n in order. Thus, it is clear that the Ω -type of $S_n^{(0)}(\mathbf{Z}_p)$ is bounded above by the Ω -type of the free pro- p group $\Gamma = \Gamma_K$ which is described in corollary 3.2.2. Recall from section 3.2 that $\text{Gal}(M/\mathbf{Q})$ is isomorphic to a semidirect product $\Gamma \rtimes \Omega$. This is how one makes Γ into an Ω group. By proposition 2.1.1, we can choose a topological generating set $\gamma_1, \dots, \gamma_r$ for Γ consisting of Ω -elements, where $\frac{1}{2}[K : \mathbf{Q}] + 1$. We have $n \leq r$. Choose the indexing so that γ_i is a χ_i -element for $1 \leq i \leq n$.

We can define a surjective homomorphism $\sigma_0 : \Gamma \rightarrow S_n^{(0)}(\mathbf{Z}_p)$ by mapping γ_i to s_i for $1 \leq i \leq n$ and mapping the γ_i 's for $i > n$ (if there are any) to I_n . It is clear that σ_0 is an Ω -homomorphism. Therefore, we can extend σ_0 to a surjective homomorphism from $\Gamma \rtimes \Omega$ to $S_n^{(0)}(\mathbf{Z}_p) \rtimes \Omega$. This then gives us a homomorphism from ρ_0 from $\text{Gal}(M/\mathbf{Q})$ to $GL_n(\mathbf{Z}_p)$ whose image contains $S_n^{(0)}(\mathbf{Z}_p)$. smallskip

Consider the representation $\rho = \rho_0 \otimes \kappa$ of $\text{Gal}(M/\mathbf{Q})$. Denote $M^{\ker(\rho_0)}$ by $\mathbf{Q}(\rho_0)$. Thus, $\text{Gal}(\mathbf{Q}(\rho_0)/\mathbf{Q})$ is isomorphic to the image of ρ_0 , a p -adic Lie group whose Lie algebra is \mathfrak{sl}_n . It follows that the maximal abelian quotient of $\text{Gal}(\mathbf{Q}(\rho_0)/\mathbf{Q})$ is finite. The field $M^{\ker(\kappa)}$ is just the cyclotomic \mathbf{Z}_p -extension \mathbf{Q}_∞ of \mathbf{Q} . Since \mathbf{Q}_∞ is an abelian extension of \mathbf{Q} , it follows that $\mathbf{Q}(\rho_0) \cap \mathbf{Q}_\infty$ is a finite extension of \mathbf{Q} . Let $F = \mathbf{Q}(\rho_0)\mathbf{Q}_\infty$. Both ρ_0 and κ can be regarded as representations of $\text{Gal}(F/\mathbf{Q})$. The restrictions of ρ and ρ_0 to $\text{Gal}(F/\mathbf{Q}_\infty)$ coincide and their image contains an open subgroup of $SL_n(\mathbf{Z}_p)$. On the other hand, the restriction of ρ to $\text{Gal}(F/\mathbf{Q}(\rho_0))$ coincides with the restriction of κ , viewed as having its values in the group $\mathbf{Z}_p^\times I_n$ of scalar matrices in $GL_n(\mathbf{Z}_p)$. The image will be an open subgroup of $\mathbf{Z}_p^\times I_n$. Thus, the image of ρ contains open subgroups of both $SL_n(\mathbf{Z}_p)$ and $\mathbf{Z}_p^\times I_n$, and hence must indeed be an open subgroup of $GL_n(\mathbf{Z}_p)$. ■

Proposition 6.1.2. *Under the assumptions of proposition 6.1.1, there exists an uncountable collection of homomorphisms ρ_0 with the stated properties and such that the corresponding kernels are distinct.*

Proof. Assume that K , p , and n satisfy the assumptions in proposition 6.1.1. Fix a choice of χ_1, \dots, χ_n and define $\omega : \Omega \rightarrow \Theta_n$ as in the proof. Thus, $S_n^{(0)}(\mathbf{Z}_p)$ can be regarded as an

Ω -group. One obtains a ρ_0 for each choice of a surjective Ω -homomorphism σ_0 from Γ to $S_n^{(0)}(\mathbf{Z}_p)$. Fix a topological generating set $\gamma_1, \dots, \gamma_r$ for Γ as in the proof of proposition 6.1.1. We continue to let s_1, \dots, s_n be the topological generators for $S_n^{(0)}(\mathbf{Z}_p)$ given in (8). Thus, $\{s_1, \dots, s_{n-1}\}$ is a topological generating set for $U_n(\mathbf{Z}_p)$. We will assume that σ_0 is defined by mapping γ_i to s_i for $1 \leq i \leq n$ and by mapping the remaining generators γ_i for $i > n$ (if r exceeds n) to the identity element I_n of $S_n^{(0)}(\mathbf{Z}_p)$.

If ψ is any Ω -automorphism of Γ_K , then $\sigma \circ \psi$ will be another surjective Ω -homomorphism from Γ_K to $S_n^{(0)}(\mathbf{Z}_p)$. We have

$$\ker(\sigma \circ \psi) = \psi^{-1}(\ker(\sigma)) \quad .$$

For simplicity, we will restrict attention to automorphisms ψ of the following special form:

$$(9) \quad \psi(\gamma_i) = \gamma_i^{a_i} \quad \text{for } 1 \leq i \leq n, \quad \psi(\gamma_i) = \gamma_i \quad \text{for } i > n \quad ,$$

where the a_i 's are in \mathbf{Z}_p^\times . Any such automorphism is clearly an Ω -automorphism. We refer to a_1, \dots, a_n as the parameters for ψ . Since Γ_K is free, any choice of a_1, \dots, a_n will determine such an automorphism ψ of Γ_K . Note that $\sigma \circ \psi$ also maps the γ_i 's for $i > n$ to I_n .

Suppose that ψ' is another automorphism of Γ of the form (9) and that the corresponding parameters are a'_1, \dots, a'_n . We will prove that

$$\ker(\sigma \circ \psi) = \ker(\sigma \circ \psi') \quad \iff \quad \prod_{i=1}^n a_i = \prod_{i=1}^n a'_i$$

and hence that there are indeed uncountably many distinct kernels for the homomorphisms $\sigma \circ \psi$. In effect, we are just replacing one set of topological generators for Γ_K by other choices, each consisting of Ω -elements. We thereby get many ρ_0 's and uncountably many distinct kernels.

One easily reduces to the case where ψ' is the identity automorphism of Γ_K , i.e., where $a'_i = 1$ for $1 \leq i \leq n$. Thus, we must show that $\sigma \circ \psi$ and σ have the same kernel if and only if $\prod_{i=1}^n a_i = 1$. To show this, assume first that the product of the a_i 's is 1. We can then define $d_1, \dots, d_n \in \mathbf{Z}_p^\times$ such that

$$a_1 = d_1 d_2^{-1}, \quad . \quad . \quad . \quad , \quad a_{n-1} = d_{n-1} d_n^{-1}, \quad a_n = d_n d_1^{-1} \quad .$$

Conjugating by the matrix $D = \sum_{i=1}^n d_i E_{ii}$ defines an automorphism δ of $S_n^{(0)}(\mathbf{Z}_p)$. We have $\delta(s_i) = s_i^{a_i}$ for $1 \leq i \leq n$. This follows from (6). It is then clear that

$$(10) \quad \sigma \circ \psi = \delta \circ \sigma$$

and therefore $\sigma \circ \psi$ and σ indeed have the same kernel.

For the converse, note that if $\sigma \circ \psi$ and σ have the same kernel, then $\ker(\sigma)$ is fixed by ψ . Thus ψ will induce an automorphism on the quotient group $\Gamma_K/\ker(\sigma)$, and hence on the group $S_n^{(0)}(\mathbf{Z}_p)$. Equation (10) holds by definition. Therefore, if a_1, \dots, a_n are the parameters for ψ , then we have

$$\delta(s_i) = s_i^{a_i}$$

for $1 \leq i \leq n$. We will show that $\prod_{i=1}^n a_i = 1$. By composing δ with the automorphism induced by a suitable diagonal matrix D , one easily reduces to the case where a_1, \dots, a_{n-1} are all 1's. Letting $a = a_n$, it then suffices to show that $a = 1$.

We are now assuming that δ fixes s_1, \dots, s_{n-1} and that $\delta(s_n) = s_n^a$. Thus, δ fixes the elements of $U_n(\mathbf{Z}_p)$. Proposition 5.3.1 implies that $C_n^{(0)}(p)$ has a topological generating set consisting of conjugates of $s_n = I_n + pE_{n1}$ by elements of $U_n(\mathbf{Z}_p)$. This follows from the facts that the Frattini subgroup of $C_n^{(0)}(p)$ is $C_n^{(0)}(p^2)$ and that there is a $U_n(\mathbf{F}_p)$ -equivariant isomorphism of $C_n^{(0)}(p)/C_n^{(0)}(p^2)$ to the additive group $M_n^{(0)}(\mathbf{F}_p)$. It is clear that if $u \in U_n(\mathbf{Z}_p)$ and if $t = us_nu^{-1}$, then $\delta(t) = t^a$. Therefore, $C_n^{(0)}(p)$ has a topological generating set consisting of elements c_j , where $1 \leq j \leq n^2 - 1$, such that $\delta(c_j) = c_j^a$ for all j 's.

We will use theorems 4.3.1, 5.3.2, and corollary 9.23 from [DSMS]. They imply that $C_n^{(0)}(p)$ is a p -adic analytic group and that its elements can be uniquely expressed in the form

$$\prod_{j=1}^{n^2-1} c_j^{x_j}$$

where the x_j 's are in \mathbf{Z}_p and can be taken as the coordinates defining the analytic structure on $C_n^{(0)}(p)$. The effect of applying δ to such an element is to multiply the corresponding coordinates by a . Hence δ is an analytic automorphism of $C_n^{(0)}(p)$. We then get an automorphism \mathfrak{d} of the Lie algebra \mathfrak{sl}_n for $C_n^{(0)}(p)$, a Lie algebra over \mathbf{Q}_p . For each j , the subgroup $\overline{\langle c_j \rangle}$ of $C_n^{(0)}(p)$ is a 1-dimensional analytic subgroup on which δ acts by the map $c \rightarrow c^a$. Thus \mathfrak{d} acts on the corresponding 1-dimensional subalgebra of \mathfrak{sl}_n as multiplication by a . Since \mathfrak{d} is \mathbf{Q}_p -linear and those subalgebras generate \mathfrak{sl}_n as a \mathbf{Q}_p -vector space, it follows that \mathfrak{d} acts as multiplication by a on \mathfrak{sl}_n and therefore on the Lie subalgebra \mathfrak{u}_n corresponding to $U_n(\mathbf{Z}_p)$. Since δ acts trivially on all of $U_n(\mathbf{Z}_p)$, \mathfrak{d} will act trivially on \mathfrak{u}_n . It follows that $a = 1$. ■

Remark 6.1.3. Following the notation in the proof of proposition 6.1.2, suppose that σ and σ' are two surjective homomorphisms from Γ_K to $S_n^{(0)}(\mathbf{Z}_p)$ and that $\ker(\sigma) \neq \ker(\sigma')$. Then $\ker(\sigma)\ker(\sigma')$ is a normal subgroup of Γ_K and the corresponding quotient group is

isomorphic to a proper quotient group of $S_n^{(0)}(\mathbf{Z}_p)$. The Lie algebra of $S_n^{(0)}(\mathbf{Z}_p)$ is \mathfrak{sl}_n , a simple Lie algebra over \mathbf{Q}_p . One shows easily that $S_n^{(0)}(\mathbf{Z}_p)$ has no nontrivial finite, normal subgroups. Thus, a closed normal subgroup of $S_n^{(0)}(\mathbf{Z}_p)$ must have finite index. In particular, $\ker(\sigma)\ker(\sigma')$ has finite index in Γ_K . Therefore, the intersection of the fields cut out by the representations σ and σ' must be a finite extension of K . If one constructs representations ρ and ρ' of $G_{\mathbf{Q}}$ from σ and σ' as in proposition 6.1.1, so that their images are open, then the intersection of the fields cut out by ρ and ρ' will be a finite extension of \mathbf{Q}_{∞} . \diamond

Remark 6.1.4. It is natural to ask whether the uncountable family of representations ρ constructed in the proof of proposition 6.1.1 includes some representations having nice arithmetic properties at p . Could one make the construction so that the restriction of ρ to a decomposition subgroup is crystalline or Hodge-Tate, for example? We don't see how to deal with such questions. The difficulties become clear by considering two extreme cases.

Suppose first that there is just one prime \mathfrak{p} of K lying over p , where K satisfies the assumptions in proposition 6.1.1. Suppose also that p doesn't divide the class number of K . Then one sees easily that \mathfrak{p} is totally ramified in M/K and therefore that Γ_K can be identified with $\text{Gal}(M_{\mathfrak{p}}/K_{\mathfrak{p}})$, where $M_{\mathfrak{p}}$ is a certain pro- p extension of $K_{\mathfrak{p}}$. However, we don't see any way to identify that extension. There may indeed be n -dimensional representations of the local Galois group $G_{K_{\mathfrak{p}}}$ with open image which have some nice properties (a question which we haven't examined), but how can one construct such representations so that they factor through the quotient group $\text{Gal}(M_{\mathfrak{p}}/K_{\mathfrak{p}})$.

Suppose now that p splits completely in K/\mathbf{Q} . Let \mathfrak{p} be one of the primes of K lying over p . Thus, $K_{\mathfrak{p}} = \mathbf{Q}_p$. If K is a complex, abelian extension of \mathbf{Q} , then one can show that the decomposition subgroup of Γ_K^{ab} for \mathfrak{p} is isomorphic to \mathbf{Z}_p^2 . This is a nontrivial fact. It follows as a consequence of proposition 3 in [Gr73]. Thus, the decomposition subgroup $D_{\mathfrak{p}}$ of Γ_K for a prime of M lying above \mathfrak{p} requires at least two topological generators. One can identify $D_{\mathfrak{p}}$ with $\text{Gal}(M_{\mathfrak{p}}/\mathbf{Q}_p)$, where $M_{\mathfrak{p}}$ is a certain pro- p extension of \mathbf{Q}_p . Furthermore, if one assumes that K is p -rational, then $D_{\mathfrak{p}}$ must be a free pro- p group since it is a subgroup of the free pro- p group Γ_K .

Now one can show that the Galois group $\Gamma_{\mathbf{Q}_p}$ for the maximal pro- p extension of \mathbf{Q}_p is a free pro- p group on 2 generators. Since there is a surjective homomorphism from $\Gamma_{\mathbf{Q}_p}$ to $D_{\mathfrak{p}}$, the facts mentioned above imply that such a homomorphism is injective and hence that $M_{\mathfrak{p}}$ is precisely the maximal pro- p extension of \mathbf{Q}_p . The difficulty is that we cannot give a description of the subgroup $D_{\mathfrak{p}}$ in terms of the type of generating set for Γ_K described in proposition 3.2.1. Thus, it is not clear how to study the restrictions $\rho|_{D_{\mathfrak{p}}}$ for the representations ρ constructed in propositions 6.1.1. \diamond

Remark 6.1.5. The image of the representation ρ in proposition 6.1.1 contains $S_n(\mathbf{Z}_p)$ if n is even and $p \nmid n$. To see this, note that if n is even, then the characters χ_1, \dots, χ_n will all be odd. Referring to the proof of the proposition, one sees that the Ω -type of $\sigma_0(\Gamma) = S_n^{(0)}(\mathbf{Z}_p)$ doesn't contain χ_0 . Let $K(\sigma_0) = M^{\ker(\sigma_0)}$ and $K_\infty = K\mathbf{Q}_\infty$, which is the fixed field for $\kappa|_\Gamma$. We then have

$$K(\sigma_0) \cap K_\infty = K .$$

Therefore, the image of $\text{Gal}(M/K_\infty)$ under σ_0 , and hence under ρ , will still be $S_n^{(0)}(\mathbf{Z}_p)$. Thus, the image of ρ contains $S_n^{(0)}(\mathbf{Z}_p)$. It then suffices to show that the image of $\det(\rho)$ contains $1 + p\mathbf{Z}_p$. However, $\kappa(\Gamma) = \kappa(\ker(\sigma_0))$ is $1 + p\mathbf{Z}_p$. The restriction of ρ to $\ker(\sigma_0)$ is just a direct sum of n copies of κ . The image under the determinant map is $1 + p\mathbf{Z}_p$ since $p \nmid n$. \diamond

6.2. Finding suitable character sets. Now we discuss the existence of a set of characters χ_1, \dots, χ_n with the properties stated in the above proposition. Suppose first that K is a cyclic extension of \mathbf{Q} and that K is complex. Then $[K : \mathbf{Q}] = 2g$ for some g . We have $|\widehat{\Omega}_{\text{odd}}| = g$. Assume that $g \geq 2$. Consider pairs of odd characters $\{\chi, \chi^{-1}\}$, where $\chi^{-1} \neq \chi$. The number of such pairs is $[g/2]$. Thus, if n is even and $n \leq 2[g/2]$, then we can take $n/2$ such pairs to obtain n distinct, odd characters whose product is χ_0 . If n is odd, then we can choose one of the characters to be χ_0 and choose the other characters in pairs as above. We then obtain a suitable set of n characters if $n - 1 \leq 2[g/2]$. In both cases, the inequality we need for n can be stated as $[n/2] \leq g/2$. Thus, we obtain the following result.

Proposition 6.2.1. *Suppose that $n \geq 2$. Suppose that K is a complex, cyclic extension of \mathbf{Q} , that $[K : \mathbf{Q}]$ divides $p - 1$, that K is p -rational, and that $[K : \mathbf{Q}] \geq 4[n/2]$. Then there exist continuous homomorphisms ρ_0 and ρ having the properties stated in proposition 6.1.1.*

Proposition 1.1 in the introduction is the special case $K = \mathbf{Q}(\mu_p)$. The assumption there is that p is a regular prime. Hence K is p -rational by proposition 4.3.1. However, even if p is irregular, the construction sometimes works. As an example, suppose that $p = 37$. Then the torsion subgroup of $(\Gamma_K^{ab})^{e_\chi}$ is nontrivial for exactly one χ , namely $\chi = \varepsilon^{32}$ where ε denotes the character giving the action of $\text{Gal}(K/\mathbf{Q})$ on μ_p . It follows from the discussion in remark 3.2.4 that the unique subfield K' of K such that $[K' : \mathbf{Q}] = 12$ is p -rational. Thus, one can apply proposition 6.1.3 for $p = 37$ to the field K' provided that $2 \leq n \leq 7$.

Another special case is $K = \mathbf{Q}(\mu_5)$. Since $[K : \mathbf{Q}] = 4$, we assume that $p \equiv 1 \pmod{4}$. Except for the seemingly rare primes p for which K fails to be p -rational, one can then apply proposition 6.1.3, taking n to be 2 or 3. In particular, one obtains representations $\rho : G_{\mathbf{Q}} \rightarrow GL_3(\mathbf{Z}_p)$ for an extremely large set of primes, including all primes $p < 10,000$

such that $p \equiv 13$ or $17 \pmod{20}$ and all primes $p < 3 \times 10^9$ such that $p \equiv 1$ or $9 \pmod{20}$.

Now consider the case where K is a compositum of quadratic fields. Thus, Ω is an elementary abelian 2-group. The exponent of Ω certainly divides $p - 1$. We prove the following result.

Proposition 6.2.2. *Suppose that K is complex and that $\Omega = \text{Gal}(K/\mathbf{Q})$ is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^t$, where $t \geq 4$. Suppose also that $4 \leq n \leq 2^{t-1} - 3$. Then one can find distinct characters χ_1, \dots, χ_n in $\widehat{\Omega}_{\text{odd}} \cup \{\chi_0\}$ whose product is χ_0 . Consequently, if we also assume that K is p -rational, then there exists continuous homomorphisms ρ_0 and ρ having the properties stated in proposition 6.1.1.*

Proof. Let $\widehat{\Omega}_{\text{ev}}$ denote the subgroup of $\widehat{\Omega}$ consisting of even characters, which has order 2^{t-1} . Let $m = 2\lceil n/2 \rceil$. Then m is even and $4 \leq m \leq n$. We will show that there exists distinct elements $\varphi_1, \dots, \varphi_m \in \widehat{\Omega}_{\text{ev}}$ whose product is χ_0 . If ψ is any element of $\widehat{\Omega}_{\text{odd}}$, then one can take $\chi_i = \psi\varphi_i$ for $1 \leq i \leq m$. These χ_i 's are distinct elements of $\widehat{\Omega}_{\text{odd}}$ and their product is χ_0 since $\psi^m = \chi_0$. If n is even, then $n = m$, and the stated result follows. If n is odd, then $n = m + 1$. We then take χ_n to be χ_0 .

To show the existence of $\varphi_1, \dots, \varphi_m$, assume first that $4|m$. Let Ξ be a subgroup of $\widehat{\Omega}_{\text{ev}}$ of order 4. Any coset of Ξ consists of four characters whose product is χ_0 . Thus, we can just choose the φ_i 's so that $\{\varphi_1, \dots, \varphi_m\}$ is a union of $m/4$ distinct cosets of Ξ in $\widehat{\Omega}_{\text{ev}}$.

On the other hand, if $4 \nmid m$, then the inequalities show that $t \geq 5$. Thus, $[\widehat{\Omega}_{\text{ev}} : \Xi] \geq 4$. The bound on n corresponds to the inequality $6 \leq m \leq 2^{t-1} - 6$. First consider $m = 6$. Suppose that the nontrivial elements of Ξ are ξ_1, ξ_2 , and ξ_3 . Suppose that φ and φ' belong to distinct, nontrivial cosets of Ξ in $\widehat{\Omega}_{\text{ev}}$. Then

$$A = \{ \xi_1, \xi_2, \varphi\xi_1, \varphi\xi_3, \varphi'\xi_2, \varphi'\xi_3 \}$$

has cardinality m and the product of the characters in A is indeed χ_0 . Those characters belong to a union of three of the cosets of Ξ . If $m > 6$, then one can form a set $A \cup B$, where B is a union of $(m - 6)/4$ of the remaining cosets of Ξ in $\widehat{\Omega}_{\text{ev}}$. The product of the elements in $A \cup B$ will again be χ_0 . This will settle all the m 's in the indicated range. ■

Remark 6.2.3. If K is a compositum of quadratic fields and $t \geq 3$, then one can simply take $\{\chi_1, \dots, \chi_n\}$ to be either $\widehat{\Omega}_{\text{odd}}$ or $\widehat{\Omega}_{\text{odd}} \cup \{\chi_0\}$. The requirements in proposition 6.1.1 are then satisfied for $n = 2^{t-1}$ or $n = 2^{t-1} + 1$, respectively. Thus, if K is p -rational, then one obtains homomorphisms ρ_0 and ρ with the properties in proposition 6.1.1 for those values of n too.

For the special case $t = 5$, we gave examples of suitable compositums of quadratic fields when $p = 3$ and $p = 5$ in section 4. Thus, using those specific K 's, we obtain representations $\rho : G_{\mathbf{Q}} \rightarrow GL_n(\mathbf{Z}_p)$ with an open image for both of those primes when $4 \leq n \leq 13$ and for $n = 16$ and $n = 17$ too. Using the example for $p = 3$ with $t = 6$, one obtains such ρ 's for $4 \leq n \leq 29$ and for $n = 32$ and 33 . If one grants conjecture 4.2.1, then proposition 6.1.1 will give such representations for all pairs (n, p) , where $p \geq 3$ and $n \geq 4$.

For $n = 2$, the requirements that $\chi_1\chi_2 = \chi_0$ and $\chi_1 \neq \chi_2$ imply that χ_1 and χ_2 have order at least 3. Similarly, if $n = 3$, the requirements on χ_1, χ_2 , and χ_3 imply that one of those three characters is χ_0 and the other two have order at least 3. Thus, compositums of quadratic fields will not work in these cases. However, if $p > 3$, then one can apply proposition 6.1.1 for $n = 2$ or $n = 3$ provided that one can find a cyclic extension K of \mathbf{Q} with the following two properties: (i) K is complex and p -rational, (ii) the degree $[K : \mathbf{Q}]$ is at least 4 and divides $p - 1$. It is reasonable to conjecture that such a field K should exist for any prime p . The remaining cases are $(n, p) = (2, 3)$ and $(n, p) = (3, 3)$, both of which resist the approach of this paper. Of course, elliptic curves give many examples of 2-dimensional representations over \mathbf{Z}_3 with open image. We haven't found a way to construct 3-dimensional representations over \mathbf{Z}_3 with open image. \diamond

7 Examples with irreducible residual representation.

Suppose that K is a finite Galois extension of \mathbf{Q} . We will assume in this section that K is totally complex and that $\Omega = \text{Gal}(K/\mathbf{Q})$ has order prime to p . We continue to assume that p is an odd prime. As before, let M denote the maximal pro- p extension of K which is unramified at all $\ell \notin \Sigma_p$. Let $\Gamma = \text{Gal}(M/K)$. We will also assume that K is p -rational in the main result and the illustrations in this section. Consequently, $\Gamma = \text{Gal}(M/K)$ will be a free pro- p group. We identify Ω with a subgroup of $\text{Gal}(M/\mathbf{Q})$. Then Γ becomes an Ω -group and $\text{Gal}(M/\mathbf{Q})$ is isomorphic to the corresponding semidirect product $\Gamma \rtimes \Omega$.

Suppose that \mathcal{F} is a finite extension of \mathbf{Q}_p , \mathfrak{m} is the maximal ideal in the ring of integers \mathcal{O} of \mathcal{F} , and $\mathfrak{f} = \mathcal{O}/\mathfrak{m}$ is the corresponding residue field. Let $\mathcal{R}_{\mathcal{F}}(\Omega)$ and $\mathcal{R}_{\mathfrak{f}}(\Omega)$ denote the Grothendieck groups for representations of Ω over \mathcal{F} and \mathfrak{f} , respectively. Then the natural map $\mathcal{R}_{\mathcal{F}}(\Omega) \rightarrow \mathcal{R}_{\mathfrak{f}}(\Omega)$ is an isomorphism. (See the references to [Ser] cited in remark 2.2.1.) The map is defined as follows. If ω is a representation of Ω over \mathcal{F} , then one can realize ω over \mathcal{O} . Let $\bar{\omega}$ denote the reduction of ω modulo \mathfrak{m} . The image of the isomorphism class of ω is defined to be the isomorphism class of $\bar{\omega}$ as an \mathfrak{f} -representation space for Ω , which is well-defined because $|\Omega|$ is not divisible by p . If ω_1 and ω_2 are arbitrary \mathcal{F} -representations

of Ω , then ω_1 is a direct summand in ω_2 if and only if $\bar{\omega}_1$ is a direct summand in $\bar{\omega}_2$. All finite-dimensional representations of Ω over \mathcal{F} and \mathfrak{f} are completely reducible. In particular, note that if ω is an absolutely irreducible representation of Ω over \mathbf{Q}_p , then $\bar{\omega}$ is an absolutely irreducible representation of Ω over \mathbf{F}_p .

As before, let Ω_∞ be the decomposition subgroup for an infinite prime of K , a subgroup of Ω of order 2, and let ε_1 be the nontrivial character of Ω_∞ , regarded as a character with values in \mathbf{Z}_p^\times . Then $\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1)$ is a representation of Ω over \mathbf{Q}_p of degree $\frac{1}{2}[K : \mathbf{Q}]$. The Frobenius Reciprocity Law implies that if ω is an absolutely irreducible representation of Ω , then the multiplicity of ω in $\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1)$ (extending scalars if necessary) coincides with the multiplicity of ε_1 in $\omega|_{\Omega_\infty}$. Thus, that multiplicity is positive unless $\Omega_\infty \subseteq \ker(\omega)$, i.e., unless ω factors through $\text{Gal}(K'/\mathbf{Q})$, where K' is a totally real Galois extension of \mathbf{Q} contained in K .

7.1. The basic proposition. The result below is a straightforward consequence of proposition 2.3.1. We will let ω_0 denote the trivial representation of Ω in this section. Note that for any representation ω of Ω over a field \mathcal{F} , the representation $\omega \otimes_{\mathcal{F}} \check{\omega}$ contains ω_0 with positive multiplicity. That multiplicity is 1 if and only if ω is absolutely irreducible. We will write the above tensor product more simply as $\omega \otimes \check{\omega}$.

Proposition 7.1.1. *In addition to the above assumptions, suppose that K is p -rational. Let ω be a representation of Ω over \mathbf{Q}_p of degree n . Assume that $\omega \otimes \check{\omega}$ is a direct summand in $\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1) \oplus \omega_0$. Then there exists a representation $\rho : \text{Gal}(M/\mathbf{Q}) \rightarrow GL_n(\mathbf{Z}_p)$ with open image such that $\bar{\rho}$ is isomorphic to $\bar{\omega}$.*

The assumption about the tensor product implies that ω is absolutely irreducible. This is so because Frobenius reciprocity implies that ω_0 is not a constituent in $\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1)$ and hence occurs with multiplicity 1 in $\omega \otimes \check{\omega}$. Therefore, since Ω has order prime to p , $\bar{\omega}$ will also be absolutely irreducible.

Proof. We can realize ω as a homomorphism from Ω to $GL_n(\mathbf{Z}_p)$. As described in section 5.6, the pro- p group $C_n(p)$ then becomes an Ω -group. It is clear that there is a homomorphism from the corresponding semidirect product $C_n(p) \rtimes \Omega$ to $GL_n(\mathbf{Z}_p)$ whose image contains $C_n(p)$ and is therefore an open subgroup of $GL_n(\mathbf{Z}_p)$. The assumptions together with proposition 3.2.1, remark 3.2.3, and the discussion in section 5.6 imply that $\widetilde{C_n(p)}$ is a direct summand in $\widetilde{\Gamma}$. Proposition 2.3.1 then implies that there is a surjective Ω -homomorphism from Γ to $C_n(p)$. Consequently, there is a surjective homomorphism from $\text{Gal}(M/\mathbf{Q})$ (which is isomorphic to $\Gamma \rtimes \Omega$) to $C_n(p) \rtimes \Omega$, and hence indeed to an open subgroup of $GL_n(\mathbf{Z}_p)$. ■

7.2. The deformation theory point of view. Let $G = \text{Gal}(M/\mathbf{Q})$. Suppose that ω satisfies the hypotheses in proposition 7.1.1. Then the \mathbf{F}_p -representation $\bar{\omega}$ of Ω is absolutely irreducible. There exists a universal deformation ring R for the pair G and $\bar{\omega}$. Thus, R is a complete Noetherian local ring with residue field \mathbf{F}_p and there exists a continuous representation $\rho_{univ} : G \rightarrow GL_n(R)$ whose residual representation is isomorphic to $\bar{\omega}$. A continuous ring homomorphism $\varphi : R \rightarrow \mathbf{Z}_p$ gives rise to a continuous representation $\rho_\varphi : G \rightarrow GL_n(\mathbf{Z}_p)$ with residual representation isomorphic to $\bar{\omega}$. Similarly, if we have such a homomorphism $\psi : R \rightarrow \mathbf{Z}/p^2\mathbf{Z}$, we obtain a representation $\rho_\psi : G \rightarrow GL_n(\mathbf{Z}/p^2\mathbf{Z})$.

Suppose that the hypothesis concerning $\omega \otimes \tilde{\omega}$ in proposition 7.1.1 is satisfied. As in the proof of the proposition, it follows that there is a surjective Ω -homomorphism from $\tilde{\Gamma}$ to $\widetilde{C_n(p)}$. Now $\widetilde{C_n(p)}$ can be identified with a subgroup of $GL_n(\mathbf{Z}/p^2\mathbf{Z})$, namely the kernel of the map $GL_n(\mathbf{Z}/p^2\mathbf{Z}) \rightarrow GL_n(\mathbf{Z}/p\mathbf{Z})$. The homomorphism ω induces a homomorphism of Ω into $GL_2(\mathbf{Z}/p^2\mathbf{Z})$. Consequently, there exists a homomorphism from $\widetilde{C_n(p)} \rtimes \Omega$ to $GL_n(\mathbf{Z}/p^2\mathbf{Z})$ whose image contains $\widetilde{C_n(p)}$.

Recall that L is the extension of K contained in M such that $\text{Gal}(L/K) \cong \tilde{\Gamma}$. Now $\text{Gal}(L/\mathbf{Q}) \cong \tilde{\Gamma} \rtimes \Omega$ and hence there is a surjective homomorphism from $\text{Gal}(L/\mathbf{Q})$ to $\widetilde{C_n(p)} \rtimes \Omega$. Thus, we obtain a homomorphism σ from $\text{Gal}(L/\mathbf{Q})$ to $GL_n(\mathbf{Z}/p^2\mathbf{Z})$ whose image contains $\widetilde{C_n(p)}$. The corresponding residual representation is isomorphic to $\bar{\omega}$. We can regard σ as a representation of G over the ring $\mathbf{Z}/p^2\mathbf{Z}$. Therefore, there must be a continuous, surjective homomorphism $\psi : R \rightarrow \mathbf{Z}/p^2\mathbf{Z}$ such that $\rho_\psi = \sigma$. Furthermore, if there exists a continuous \mathbf{Z}_p -algebra homomorphism $\varphi : R \rightarrow \mathbf{Z}_p$ lifting ψ , then we obtain a representation $\rho_\varphi : G \rightarrow GL_n(\mathbf{Z}_p)$ whose residual representation is isomorphic to $\bar{\omega}$ and whose reduction modulo p^2 is σ . It follows from **BBT** that the image of ρ_φ contains $C_n(p)$ and hence is an open subgroup of $GL_n(\mathbf{Z}_p)$.

The above remarks show that if one makes the assumptions that $\omega \otimes \tilde{\omega}$ is a direct summand in $\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1) \oplus \omega_0$ and that every continuous \mathbf{Z}_p -algebra homomorphism $\psi : R \rightarrow \mathbf{Z}/p^2\mathbf{Z}$ can be lifted to a continuous \mathbf{Z}_p -algebra homomorphism $\varphi : R \rightarrow \mathbf{Z}_p$, then one will obtain continuous representations $\rho : G \rightarrow GL_n(\mathbf{Z}_p)$ with open image and residual representation isomorphic to $\bar{\omega}$. It is not clear what assumptions about R guarantee the existence of such liftings. If it happens that R is isomorphic to a formal power series ring $\mathbf{Z}_p[[X_1, \dots, X_t]]$ for some $t \geq 0$, then it is clear that the above lifting property holds. One sufficient condition for R to have that structure is given in proposition 2 in [Maz]. It suffices to have $H^2(G, \text{ad}(\bar{\omega})) = 0$. This is the so-called unobstructed case in deformation theory.

Recall that K is p -rational if and only if $H^2(\Gamma, \mathbf{Z}/p\mathbf{Z}) = 0$. By Shapiro's lemma, another equivalent statement is that $H^2(G, \mathbf{F}_p[\Omega]) = 0$, where $\mathbf{F}_p[\Omega]$ is the regular representation of Ω , regarded as a G -module. This vanishing statement is in turn equivalent to the vanish-

ing of $H^2(G, \alpha)$ for all $\alpha \in \text{Irr}_{\mathbf{F}_p}(\Omega)$. In particular, if K is p -rational, then it follows that $H^2(G, ad(\bar{\omega})) = 0$ since $ad(\bar{\omega})$ is isomorphic to a direct sum of irreducible \mathbf{F}_p -representation spaces. Sometimes, it turns out that the vanishing of $H^2(G, ad(\bar{\omega}))$ and of $H^2(G, \mathbf{F}_p[\Omega])$ are equivalent. As an example, suppose that Ω is the simple group of order 168, whose representation theory will be discussed below, and that ω is either the irreducible representation of degree 7 or of degree 8. Then every irreducible representation of Ω is a constituent in $\omega \otimes \check{\omega}$, as we point out below. It then follows that every α in $\text{Irr}_{\mathbf{F}_p}(\Omega)$ occurs as a constituent in $ad(\bar{\omega})$. The vanishing of $H^2(G, ad(\bar{\omega}))$ and of $H^2(G, \mathbf{F}_p[\Omega])$ are indeed equivalent. Consequently, the field K is p -rational if and only if $H^2(G, ad(\bar{\omega})) = 0$.

As a simpler example, suppose that $\Omega = \text{Gal}(K/\mathbf{Q})$ is isomorphic to S_3 and that ω is the 2-dimensional irreducible representation of Ω . Assume that $p \geq 5$. Then all three elements of $\text{Irr}_{\mathbf{F}_p}(\Omega)$ are constituents in $ad(\bar{\omega})$. Hence K is p -rational if and only if $H^2(G, ad(\bar{\omega}))$ vanishes. In this special case, that vanishing means that R is isomorphic to a formal power series ring over \mathbf{Z}_p in either one or three variables, depending on whether K is totally real or totally complex. In [Maz], Mazur considers certain examples of totally complex S_3 -extensions K of \mathbf{Q} which he calls “*special*”. These extensions correspond to primes p of the form $p = 27 + 4a^3$. For each such prime p , Let K be the splitting field over \mathbf{Q} for the polynomial $x^3 + ax + 1$. There are eighteen such primes $p < 10^6$ and the field K turns out to be p -rational for each of them.

7.3. An illustration. We discuss the example mentioned in the introduction. Thus, we will suppose that $\Omega = \text{Gal}(K/\mathbf{Q})$ is isomorphic to the symmetric group S_{n+1} for some n . It is known that such totally complex Galois extensions K/\mathbf{Q} exist for all $n \geq 0$. We fix an isomorphism. Suppose that $n \geq 2$. Then S_{n+1} has an absolutely irreducible representation of degree n , a direct summand in the obvious permutation representation of degree $n + 1$. We will let ω_n be the corresponding representation of Ω . All the representations of the symmetric groups are self-dual. In particular, $\check{\omega}_n \cong \omega_n$.

Proposition 7.3.1. *If $n = 2$ or $n \geq 4$, then the representation $\omega_n \otimes \omega_n$ is a direct summand in $\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1) \oplus \omega_0$. If $n = 3$, this statement is true if the unique quadratic subfield of K is imaginary.*

The proof depends on the lemma below. We will use various results about the representation theory of S_{n+1} which can be found in [JaKe]. We think of S_{n+1} as the group of permutations of a set $X_{n+1} = \{x_1, \dots, x_{n+1}\}$. First of all, the absolutely irreducible representations of symmetric groups are always realizable over \mathbf{Q} . This is theorem 2.1.3 in [JaKe]. In particular, they are all self-dual. That latter fact is clear because if $g \in S_{n+1}$, then g and g^{-1} have the same cycle decomposition and hence are conjugate. This implies that the characters

of all representations of S_{n+1} are real-valued. In fact, g is conjugate to any generator of the cyclic group $\langle g \rangle$ generated by g and this implies that all these characters have values in \mathbf{Q} . The fact that the corresponding representations can be defined over \mathbf{Q} is somewhat harder to show.

The isomorphism classes of irreducible representations of S_{n+1} correspond to partitions of $n+1$ as sums of positive integers. For any such partition $n+1 = a_1 + \dots + a_t$, where $t \geq 0$, we assume that the terms are arranged so that $a_i \geq a_{i+1}$ for $1 \leq i < t$. The corresponding irreducible representation will be denoted by $[a_1, \dots, a_t]$. This notation (which is taken from [JaKe]) indicates in part that this irreducible representation is a constituent in $\text{Ind}_H^{S_{n+1}}(\mathbf{1}_H)$, where H is a subgroup of S_{n+1} isomorphic to the direct product $S_{a_1} \times \dots \times S_{a_t}$ and is defined by expressing the set X_{n+1} as a disjoint union of t subsets with cardinalities a_1, \dots, a_t . Here $\mathbf{1}_H$ is the trivial representation of H . To uniquely determine $[a_1, \dots, a_t]$, one requires also that the twist $[a_1, \dots, a_t] \otimes \text{sgn}$ is a constituent in $\text{Ind}_{H'}^{S_{n+1}}(\mathbf{1}_{H'})$, where sgn is the nontrivial character of S_{n+1}/A_{n+1} and H' is a subgroup of S_{n+1} defined just as above, but corresponding to another partition $n+1 = a'_1 + \dots + a'_t$ of $n+1$ which is specified in the following way. The original partition defines a matrix A with t rows and a_1 columns, where the i -th row has the first a_i entries equal to 1 and the remaining entries (if any) equal to 0. Thus, the total number of 1's in the matrix A is $n+1$. The second partition is defined to be the one whose corresponding matrix A' is the transpose of A . Thus, $a'_1 = t$ and $t' = a_1$.

The trivial representation of S_{n+1} corresponds to the partition with $t = 1$, and is denoted by $[n+1]$. The natural permutation representation of S_{n+1} is $\text{Ind}_{S_n}^{S_{n+1}}(\mathbf{1}_{S_n})$, where S_n is identified with the subgroup of S_{n+1} fixing x_{n+1} . That induced representation has an irreducible constituent of degree n which corresponds to the partition $n+1 = a_1 + a_2$, with $a_1 = n$, $a_2 = 1$, and is the irreducible representation $[n, 1]$. Note that $\mathbf{1}_{S_n}$ is $[n]$. We prove the following lemma:

Lemma 7.3.2. *If $n \geq 3$, then we have an isomorphism*

$$[n, 1] \otimes [n, 1] \cong [n+1] \oplus [n, 1] \oplus [n-1, 2] \oplus [n-1, 1, 1]$$

as representations of S_{n+1} . In particular, each irreducible constituent in $[n, 1] \otimes [n, 1]$ has multiplicity 1. The only irreducible constituent of degree 1 is $[n+1]$.

Although we won't need it, the degrees of the four constituents in $[n, 1] \otimes [n, 1]$ turn out to be 1, n , $\frac{1}{2}(n+1)(n-2)$, and $\frac{1}{2}n(n-1)$, respectively. One sees this by using theorem 2.3.21 in [JaKe].

Proof of the lemma. Identifying S_n with a subgroup of S_{n+1} as above, we have

$$([n, 1] \otimes [n, 1]) \oplus [n, 1] \cong ([n, 1] \oplus [n+1]) \otimes [n, 1] \cong \text{Ind}_{S_n}^{S_{n+1}}([n]) \otimes [n, 1] .$$

One sees easily from the definitions that the restriction of the natural permutation representation of S_{n+1} to the subgroup S_n is isomorphic to the direct sum $[n-1, 1] \oplus [n] \oplus [n]$. It follows that the restriction of $[n, 1]$ to S_n is isomorphic to the direct sum $[n-1, 1] \oplus [n]$. Using a standard property of induction, we have

$$\text{Ind}_{S_n}^{S_{n+1}}([n]) \otimes [n, 1] \cong \text{Ind}_{S_n}^{S_{n+1}}([n-1, 1] \oplus [n]) \cong \text{Ind}_{S_n}^{S_{n+1}}([n-1, 1]) \oplus \text{Ind}_{S_n}^{S_{n+1}}([n]) \quad .$$

The Branching Theorem, which is theorem 2.4.2 in [JaKe], gives the decomposition of $\text{Ind}_{S_n}^{S_{n+1}}(\chi)$ if χ is an irreducible representation of S_n . Suppose that χ corresponds to the partition $n = a_1 + \dots + a_t$, as above, where $t \geq 1$. We can imagine this partition of n as a partition with $t+1$ terms by setting $a_{t+1} = 0$. We can form various partitions of $n+1$ by replacing exactly one of the summands a_i by a_i+1 . We consider only the resulting partitions where the summands are in nondecreasing order. Thus, if some of the a_i 's are repeated, we need only augment the first such summand by 1. Then $\text{Ind}_{S_n}^{S_{n+1}}(\chi)$ is isomorphic to the direct sum of the irreducible representations which corresponds to the various partitions of $n+1$ obtained as just described. In particular, we have

$$\text{Ind}_{S_n}^{S_{n+1}}([n]) \cong [n+1] \oplus [n, 1], \quad \text{Ind}_{S_n}^{S_{n+1}}([n-1, 1]) \cong [n, 1] \oplus [n-1, 2] \oplus [n-1, 1, 1] \quad .$$

The first isomorphism amounts to the definition that we gave before for the irreducible representation $[n, 1]$ of S_{n+1} of degree n . The isomorphism in the lemma follows directly from the above isomorphisms. ■

Proof of the proposition. If $n = 2$, then $\Omega \cong S_3$ has three nonisomorphic irreducible representations and one checks easily that $\omega_2 \otimes \omega_2$ is isomorphic to their direct sum, each with multiplicity 1. However, $\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1) \oplus \omega_0$ is also isomorphic to that direct sum.

If $n = 3$, then $\Omega \cong S_4$ and the stated assumption about K implies that a generator of Ω_∞ corresponds to a transposition in the isomorphism. For any $n \geq 0$, the transpositions in S_{n+1} are all conjugate and generate S_{n+1} . If ω is any irreducible representation of Ω , and $\omega \neq \omega_0$, then it follows that $\Omega_\infty \not\subset \ker(\omega)$ and hence that $\omega|_{\Omega_\infty}$ contains ε_1 as a constituent. Thus, every irreducible representation of Ω is a constituent in $\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1) \oplus \omega_0$. On the other hand, lemma 7.2.2 implies that the irreducible constituents in $\omega_3 \otimes \omega_3$ have multiplicity 1. It follows that $\omega_3 \otimes \omega_3$ is indeed a direct summand in $\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1) \oplus \omega_0$.

If $n \geq 4$, then Ω has just one proper normal subgroup. We denote that subgroup by Θ . We have $[\Omega : \Theta] = 2$. Of course, Θ corresponds to the alternating group A_{n+1} under the isomorphism $\Omega \cong S_{n+1}$. There is a nontrivial representation ω_1 of Ω whose kernel is Θ . Apart from ω_0 and ω_1 , it follows that the remaining irreducible representations of Ω are

all faithful. Hence, if ω is any such representation, ε_1 must occur as a constituent in $\omega|_{\Omega_\infty}$. Frobenius reciprocity therefore implies that ω occurs as a constituent in $\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1)$. Thus, the proposition will follow if we show that each of the irreducible constituents in $\omega \otimes \omega$ has multiplicity 1 in that representation space and that ω_1 does not occur as a constituent. The latter fact is needed because it is possible to have $\Omega_\infty \subset \Theta$ and ω_1 will fail to be a constituent in $\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1)$ in that case.

Lemma 7.3.2 shows that $\omega_n \otimes \omega_n$ has four irreducible constituents and that they are indeed nonisomorphic. The representation ω_1 of Ω corresponds to the representation of S_{n+1} with kernel A_{n+1} . The corresponding partition of $n+1$ has $t = n+1$ and all summands equal to 1. This representation is $[1, \dots, 1]$ and is not isomorphic to any of the four constituents in $[n, 1] \otimes [n, 1]$. Thus, the properties of $\omega_n \otimes \omega_n$ that we need are indeed true. \blacksquare

Remark 7.3.3. If $n = 3$, then Ω contains a unique normal subgroup of order 4, the Klein 4-group, which we denote by Υ . The quotient Ω/Υ is isomorphic to S_3 . If the unique quadratic subfield of K is real, then $\Omega_\infty \subset \Upsilon$. There are five irreducible representations of Ω . Three of them factor through Ω/Υ and have degrees 1, 1, and 2. The other two have degree 3 and are faithful. Let ω_2 denote the unique irreducible 2-dimensional representation of Ω . In fact, ω_2 corresponds to the representation $[2, 2]$ of S_4 . We have $\ker(\omega_2) = \Upsilon$. Frobenius reciprocity implies that ω_2 is not a constituent in $\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1)$. However, ω_2 is a constituent in $\omega_3 \otimes \omega_3$. Therefore the assumption in proposition 7.3.1 is not satisfied in this case. \diamond

7.4. Additional illustrations. Propositions 7.1.1 and 7.3.1 provide a possible source of examples of continuous n -dimensional representations of $G_{\mathbf{Q}}$ over \mathbf{Q}_p with open image and absolutely irreducible residual representation. However, if $n \geq 3$ and p is any prime, then it would seem rather difficult to determine whether an extension K/\mathbf{Q} with $\text{Gal}(K/\mathbf{Q}) \cong S_{n+1}$ is actually p -rational. We have not made any attempt to do such a computation. If one does manage to find such a field, then one can apply proposition 7.1.1 to other irreducible representations of $\text{Gal}(K/\mathbf{Q})$ of various dimensions. We give several illustrations.

7.4.1. $\Omega \cong S_5$. Suppose that K is totally complex and is p -rational for some prime $p \geq 7$. The elements of order 2 in S_5 form two conjugacy classes, one consisting of the transpositions, the other consisting of products of two disjoint transpositions. Thus, there are two possible conjugacy classes for Ω_∞ . The unique quadratic subfield of K is imaginary when Ω_∞ corresponds to a subgroup of S_5 generated by a transposition. For the other possibility for Ω_∞ , that quadratic subfield will be real. Now S_5 has seven irreducible representations. In addition to the two one-dimensional representations factoring through S_5/A_5 , there are two of degree 4, two of degree 5, and one of degree 6, up to isomorphism. We denote the corresponding irreducible representations of Ω by ω_0 , ω_1 , $\omega_{4,1}$, $\omega_{4,2}$, $\omega_{5,1}$, $\omega_{5,2}$, and ω_6 . The

degrees of the nontrivial representations listed here are indicated by boldface subscripts. To be more precise, $\omega_{4,1}$ corresponds to $[4, 1]$, $\omega_{4,2} = \omega_{4,1} \otimes \omega_1$ corresponds to $[2, 1, 1, 1]$, $\omega_{5,1}$ corresponds to $[3, 2]$, and $\omega_{5,2} = \omega_{5,1} \otimes \omega_1$ corresponds to $[2, 2, 1]$. The trivial representation is ω_0 .

If the unique quadratic subfield of K is imaginary, then one finds that

$$\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1) \cong \omega_1 \oplus \omega_{4,1} \oplus \omega_{4,2}^3 \oplus \omega_{5,1}^2 \oplus \omega_{5,2}^3 \oplus \omega_6^3 .$$

On the other hand, if ω is any one of the irreducible representations of Ω , the decomposition of the tensor product $\omega \otimes \omega$ can be found in the table in [JaKe] starting on page 451. One finds that all of the irreducible constituents in $\omega \otimes \omega$ have multiplicity 1, except for the case $\omega = \omega_6$. If $\omega = \omega_6$, then all of the irreducible constituents in $\omega \otimes \omega$ have multiplicity 1, except for $\omega_{5,1}$ and $\omega_{5,2}$, both of which have multiplicity 2. Thus, for any irreducible ω , the hypotheses in proposition 7.1.1 are satisfied and consequently, under the assumption that $p \geq 7$ and that K is p -rational, there would then exist continuous n -dimensional representations of $G_{\mathbf{Q}}$ with open image and absolutely irreducible residual representation (isomorphic to $\bar{\omega}$) for $n = 4, 5$, and 6.

If the unique quadratic subfield of K is real, then it turns out that

$$\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1) \cong \omega_{4,1}^2 \oplus \omega_{4,2}^2 \oplus \omega_{5,1}^2 \oplus \omega_{5,2}^2 \oplus \omega_6^4 .$$

Note that ω_1 is not a constituent in this induced representation. Now it turns out that ω_1 is a constituent (with multiplicity 1) in $\omega_6 \otimes \omega_6$, but is not a constituent in $\omega \otimes \omega$ for the other irreducible representations of Ω . Thus, the hypotheses in proposition 7.1.1 are satisfied for all the irreducible representations ω of Ω , except for ω_6 . For any such ω , one would obtain a continuous representation ρ of $G_{\mathbf{Q}}$ with open image such that $\bar{\rho} \cong \bar{\omega}$, again under the assumption that K is p -rational. The dimension would be 4 or 5.

7.4.2. $\Omega \cong A_5$. Thus, Ω is the simple group of order 60. We still assume that $p \geq 7$ and that K is totally complex and p -rational. In this case, there is only one possible conjugacy class for Ω_∞ . There are five irreducible representations of Ω . In addition to ω_0 , two have degree 3, one has degree 4, and one has degree 5. The ones of degree 4 and 5 are the restrictions of representations of S_5 and hence are realizable over \mathbf{Q} . The two of degree 3 are the irreducible constituents of $\omega_6|_{A_5}$ and are realizable over the field $\mathbf{Q}(\sqrt{5})$. All of these representations are self-dual. One finds that $\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1)$ is isomorphic to the direct sum of the four nontrivial irreducible representations, all with multiplicity 2. Furthermore, if ω is any one of the irreducible representations of Ω , one finds that the hypothesis about $\omega \otimes \omega$ in proposition 7.1.1 is again satisfied. Thus, if one can find such a field K , one would then obtain continuous n -dimensional representations of $G_{\mathbf{Q}}$ over \mathbf{Q}_p with open image and

irreducible residual representation for $n = 4$ or 5 . The same thing is true for $n = 3$ if one assumes that p splits in the quadratic field $\mathbf{Q}(\sqrt{5})$.

7.4.3. $\Omega \cong S_6$. If $p \geq 7$, K is totally complex and p -rational, and $\Omega \cong S_6$, then there are three possible conjugacy classes for Ω_∞ . There are eleven irreducible representations of S_6 . Their degrees are 1, 5, 9, 10, and 16. Up to isomorphism, there are four irreducible representations of degree 5, two for each of the degrees 1, 9, and 10, and just one of degree 16. For all of these irreducible representations ω of Ω , except for the one of degree 16, and for all three possibilities for the isomorphism class of $\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1)$, one finds that the hypothesis concerning $\omega \otimes \omega$ in proposition 7.1.1 is satisfied. To verify this, one can use the above cited tables in [JaKe] as before to determine the decomposition of the representation space $\omega \otimes \omega$. The character tables on page 350 in [JaKe] together with Frobenius reciprocity determine the decomposition of $\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1)$. As a consequence, if one can find such a field K , one would then obtain continuous n -dimensional representations of $G_{\mathbf{Q}}$ with open image and irreducible residual representation for $n = 5, 9$, and 10 .

7.4.4. $\Omega \cong PSL_2(\mathbf{F}_7)$. In this final illustration, Ω is the simple group of order 168. At the end of [Ham], Hamblen discusses one such example due to W. Trinks, where K is the splitting field for $x^7 - 7x + 3$ over \mathbf{Q} . There are two absolutely irreducible representations of Ω of degree 3. Let ω be either one of them. Hamblen's main result in [Ham] can be applied to this example when $p \equiv 8 \pmod{21}$ to construct a 3-dimensional representation ρ of $G_{\mathbf{Q}}$ over \mathbf{Q}_p with open image such that $\bar{\rho} \cong \bar{\omega}$. His representation ρ is unramified outside a finite set containing $\Sigma_p \cup \{3, 7, \infty\}$. Interestingly, his construction gives a representation ρ such that $\rho(D_p)$ is upper triangular, where D_p is the decomposition subgroup of $G_{\mathbf{Q}}$ for some prime above p .

In contrast, proposition 7.1.1 can be applied only if one can verify that K is p -rational, where $p \notin \{2, 3, 7\}$. As with the other examples, we haven't attempted to do this, but we would expect that any fixed number field K will turn out to be p -rational for almost all primes p . That is, the set of exceptions should have Dirichlet density 0.

The character table for $PSL_2(\mathbf{F}_7)$ can be found on page 318 in [JaLi]. The following remarks are derived from that table. In addition to the trivial representation ω_0 , there are five isomorphism classes of absolutely irreducible representations of Ω . We denote them by $\omega_{3,1}$, $\omega_{3,2}$, ω_6 , ω_7 , and ω_8 . The two representations of degree 3 are contragredients of each other. The others are self-dual. Furthermore, there is only one conjugacy class of elements of order 2. Hence Ω_∞ is unique up to conjugacy and one finds that

$$\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1) \cong \omega_{3,1}^2 \oplus \omega_{3,2}^2 \oplus \omega_6^2 \oplus \omega_7^4 \oplus \omega_8^4 .$$

As for the tensor product occurring in proposition 7.1.1, the decomposition is as follows:

$$\begin{aligned} \omega_{3,1} \otimes \omega_{3,2} &\cong \omega_0 \oplus \omega_8, & \omega_7 \otimes \omega_7 &\cong \omega_0 \oplus \omega_{3,1} \oplus \omega_{3,2} \oplus \omega_6^2 \oplus \omega_7^2 \oplus \omega_8^2, \\ \omega_6 \otimes \omega_6 &\cong \omega_0 \oplus \omega_6^2 \oplus \omega_8^2, & \omega_8 \otimes \omega_8 &\cong \omega_0 \oplus \omega_{3,1} \oplus \omega_{3,2} \oplus \omega_6^2 \oplus \omega_7^3 \oplus \omega_8^3. \end{aligned}$$

Each of these tensor products is a direct summand in $\text{Ind}_{\Omega_\infty}^\Omega(\varepsilon_1) \oplus \omega_0$.

Except for the irreducible representations of degree 3, all of the others have rational-valued characters. Furthermore, the Schur indices over \mathbf{Q} turn out to all be 1. Hence the irreducible representations of degree 6, 7, and 8 can be realized over \mathbf{Q} and therefore over \mathbf{Q}_p for any prime p . To verify the assertion about the Schur index of an irreducible representation ω of Ω , it suffices to find a subgroup Θ of Ω and an irreducible representation θ of Θ realizable over \mathbf{Q} such that θ occurs with multiplicity 1 in $\omega|_\Theta$. Frobenius reciprocity then implies that ω occurs with multiplicity 1 in $\text{Ind}_\Theta^\Omega(\theta)$, a representation of Ω which is clearly realizable over \mathbf{Q} . The Schur index for ω over \mathbf{Q} divides that multiplicity, and hence indeed must be 1.

Let Θ be a Sylow 2-subgroup of Ω . One finds that Θ is the dihedral group of order 8. Let θ be one of the three characters of order 2 of Θ . If θ is trivial on the elements of order 4 in Θ , then one finds that θ has multiplicity 1 in the restrictions of $\omega_{3,1}$, $\omega_{3,2}$, ω_7 , and ω_8 . Thus, ω_7 and ω_8 are realizable over \mathbf{Q} . It also follows that $\omega_{3,1}$ and $\omega_{3,2}$ have Schur index 1 over the field $\mathbf{Q}(\sqrt{-7})$ and hence are realizable over that field. If one takes θ to be one of the other characters of order 2, then one finds that θ has multiplicity 1 in the restriction of ω_6 to Θ (as well as in the restrictions of ω_7 and ω_8). Hence ω_6 is also realizable over \mathbf{Q} .

Therefore, assuming that K is p -rational and that $p \geq 11$ or $p = 5$, one would obtain continuous representations ρ of $G_{\mathbf{Q}}$ of degrees 6, 7, or 8 such that the image of ρ is open and the residual representation $\bar{\rho}$ is an absolutely irreducible representation factoring through Ω . One also obtains such representations of degree 3 if one makes the additional assumption that p split in the quadratic field $\mathbf{Q}(\sqrt{-7})$.

References

- [Bos] N. Boston, *Explicit deformations of Galois representations*, Invent. Math. **103** (1991), 181-196.
- [DSMS] J. D. Dixon, M. P. F. du Sautoy, A. Mann, D. Segal, *Analytic pro- p groups*, London Math. Soc. Lecture Note Series **157**, Cambridge University Press (1991).
- [Fuj] S. Fujii, *On the maximal pro- p extension unramified outside p of an imaginary quadratic field*, Osaka J. Math. **45** (2008), 41-60.

- [Gor] D. Gorenstein, *Finite groups*, Chelsea Publ. Co. (1980).
- [Gr73] R. Greenberg, *On a certain ℓ -adic representation*, *Invent. Math.* **21** (1973), 117-124.
- [Gr1] R. Greenberg, *Iwasawa Theory, Projective Modules, and Modular Representations*, to appear in *Memoirs of the Amer. Math. Soc.*
- [Gr2] R. Greenberg, *Galois properties of elliptic curves with an isogeny*, preprint.
- [Ham] S. Hamblen, *Lifting n -dimensional Galois representations*, *Can. Jour. of Math.* **60** 2008, 1028-1049.
- [HeRi] , W. N. Herfort, L. Ribes, *On automorphisms of free pro- p -groups I*, *Proc. Amer. Math. Soc.* **108** (1990), 287-295.
- [Hub] , D. Hubbard, *The nonexistence of certain free pro- p extensions and capitulation in a family of dihedral extensions of \mathbf{Q}* , University of Washington Ph. D. thesis, 1996.
- [JaKe] G. James, A. Kerber, *The representation theory of the symmetric group*, *Encyclopedia of Mathematics and its Applications* **16** (1981), Addison-Wesley.
- [JaLi] G. James, M. Liebeck, *Representations and characters of groups*, 2001, Cambridge University Press.
- [JaNg] J. F. Jaulent, T. Nguyen Quang Do, *Corps p -rationnels, corps p -réguliers, et ramification restreinte*, *Séminaire de Théorie des Nombres de Bordeaux*, (1987-88), Exposé 10, 10-01 - 10-26.
- [Maz] B. Mazur, *Deforming Galois representations*, in *Galois Groups over \mathbf{Q}* , *Math. Sci. Res. Inst. Publ.* **16**, Springer, New York, 1989, 385-437.
- [Min] J. Minardi, *Iwasawa modules for \mathbf{Z}_p^d -extensions of algebraic number fields*, University of Washington Ph. D. thesis, 1986.
- [Mov] A. Movahhedi, *Sur les p -extensions des corps p -rationnels*, *Math. Nach.* **149** (1990), 163-176.
- [MoNg] A. Movahhedi, T. Nguyen Quang Do, *Sur l'arithmétique des corps de nombres p -rationnels*, *Prog. Math.* **81**, Birkhauser (1990), 155-200.
- [Ngu] T. Nguyen Quang Do, *Sur la \mathbf{Z}_p -torsion de certains modules Galoisien*, *Ann. Inst. Fourier* **36** (1986), 27-46.

- [NSW] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, Grundlehren der Math. Wissenschaften **323** (2000), Springer.
- [Ser] J. P. Serre, *Linear representations of finite groups*, Graduate Texts in Math. (1977), Springer.
- [Sha] I. R. Shafarevich, *Extensions with given points of ramification*, Amer. Math. Soc. Translations **59** (1966), 128-149.
- [Upt] M. G. Upton, *Galois representations attached to Picard curves*, Jour. Algebra **322** (2009), 1038-1059.
- [Was] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed. Graduate Texts in Math. Springer (1997).
- [Yam] *A note on free pro- p -extensions of algebraic number fields*, Jour. Théorie des Nombres de Bordeaux **5** (1993), 165-178.