The Density of Ramified Primes in Semisimple
\(p\)-adic Galois Representations

Chandrashekhar Khare and C. S. Rajan

1 Introduction

Let \(L\) be a number field. Consider a continuous, semisimple \(p\)-adic Galois representation
\[ \rho : G_L \rightarrow GL_m(K) \]
of the absolute Galois group \(G_L\) of \(L\) and with \(K\) a finite extension of \(Q_p\). In [R] in the case when \(n = 2\) and \(L = Q\) examples of such representations were constructed which were ramified at infinitely many primes, which had open image, and which had determinant \(\varepsilon\), the \(p\)-adic cyclotomic character (see also the last section of [KR]). We say that such representations are infinitely ramified. One may ask if in these examples of [R] the set of ramified primes is of small density.

**Theorem 1.** Let \(\rho : G_L \rightarrow GL_m(K)\) be a continuous, semisimple representation. Then the set of primes \(S_\rho\) that ramify in \(\rho\) is of density zero.

The semisimplicity assumption is crucial as, using Kummer theory (see the exercise of [S2, III-12]), one can construct examples of continuous, reducible, indecomposable representations \(\rho : G_L \rightarrow GL_2(Q_p)\) that are ramified at all primes. Note that as in [R] infinitely ramified representations, though not motivic themselves, arise as limits of motivic \(p\)-adic representations.

After Theorem 1, we know that the set of primes that are unramified in a continuous, semisimple representation \(\rho : G_L \rightarrow GL_m(K)\) is of density 1. Hence many of the results (e.g., the strong multiplicity 1 results of [Ra]), which are available in the classi-
After Theorem 1, it also makes good sense to talk of compatible systems of continuous, semisimple Galois representations in the sense of [S2] without imposing the condition that these be finitely ramified. We raise the following question.

Question 1. Given two compatible continuous, semisimple representations \( \rho : G_L \to \text{GL}_m(\mathbb{Q}_\ell) \) and \( \rho' : G_L \to \text{GL}_m(\mathbb{Q}_{\ell'}) \) with \( \ell \neq \ell' \), is the set of primes at which either \( \rho \) or \( \rho' \) ramifies finite?

## 2 Proof of theorem

### 2.1

Let \( \rho \) be as in Theorem 1. As \( \rho \) is continuous, we can regard \( \rho \) as taking values in \( \text{GL}_m(O) \), where \( O \) is the ring of integers of \( K \). We denote the maximal ideal of \( O_K \) by \( m \), and we denote by \( \rho_n \) the reduction mod \( m^n \) of \( \rho \).

We define \( S_{\rho,n} \) to be the set of primes \( q \) of \( L \) which satisfy the following conditions:

1. \( q \) is of degree 1 over \( \mathbb{Q} \) (this assumption is merely for notational convenience; we denote abusively the prime of \( \mathbb{Q} \) lying below it by \( q \));
2. \( q \) is unramified in \( \rho_1 \) and not equal to \( p \);
3. \( \rho_n|_{D_q} \) is unramified, but there exists a “lift” of \( \rho_n|_{D_q} \), with \( D_q \) the decomposition group at \( q \) corresponding to a place above \( q \) in \( \overline{Q} \), to a representation \( \overline{\rho}_q \) of \( D_q \) to \( \text{GL}_m(K) \) that is ramified at \( q \); by a lift we mean some conjugate of \( \overline{\rho}_q \) which reduces mod \( m^n \) to \( \rho_n|_{D_q} \). Note that by (2) any such lift \( \overline{\rho}_q \) factors through \( G_q \), the quotient of \( D_q \) which is the Galois group of the maximal tamely ramified extension of \( \mathbb{Q}_q \). Let \( c_{\rho,n} \) be the upper density of the set \( S_{\rho,n} \).

**Proposition 1.** Given any \( \varepsilon > 0 \), there is an integer \( N_\varepsilon \) such that \( c_{\rho,n} < \varepsilon \) for \( n > N_\varepsilon \). \( \square \)

We claim that the proposition implies Theorem 1. To see this, first observe that the primes of \( L \) which do not lie above primes of \( \mathbb{Q} \) which split in the extension \( L/\mathbb{Q} \) are of density zero. To prove the theorem, it is enough to show that given any \( \varepsilon > 0 \) the upper density of the set \( S_\rho \) of ramified primes for \( \rho \) is less than \( \varepsilon \). Consider the \( N_\varepsilon \) that the proposition provides. Further, note that in \( \rho_{N_\varepsilon} \) only finitely many primes ramify. From this it readily follows that the upper density of \( S_\rho \) is less than \( \varepsilon \). Hence we have Theorem 1. Thus it only remains to prove the proposition.

### 2.2 Tame inertia

Proposition 1 relies on the structure of the Galois group \( G_q \) of the maximal tamely
ramified extension of $\mathbb{Q}_q$. This is used to calculate the densities $c_{\rho,n}$ for large enough $n$. The concept of largeness of $n$ for our purposes is independent of the representation $\rho$ and the prime $q$ and depends only on $K$ and the dimension of the representation. Roughly, the idea of the proof of Proposition 1 is that for these large $n$ only semistable (i.e., the image of inertia is unipotent) lifts intervene in the calculation of the $c_{\rho,n}$, and the conjugacy classes in the image of $\rho_n$ of the Frobenius classes associated to the primes in $S_{\rho,n}$ lie in the $\mathbb{O}/m^n$-valued points of an analytically defined subset of $\text{im}(\rho)$ of smaller dimension.

We flesh out this idea below. We implicitly use the fact that although one cannot speak of eigenvalues of an element of $\text{GL}_m(A)$, for a general ring $A$, its characteristic polynomial makes good sense.

The group $G_q$ is topologically generated by two elements $\sigma_q$ and $\tau_q$ that satisfy the relation

$$\sigma_q \tau_q \sigma_q^{-1} = \tau_q^q$$  \hspace{1cm} (1)

and such that $\sigma_q$ induces the Frobenius on residue fields and $\tau_q$ (topologically) generates the tame inertia subgroup.

2.3 Reduction to the semistable case

**Lemma 1.** Let $\theta : G_q \to \text{GL}_m(K)$ be any continuous representation. Then the roots of the characteristic polynomial of $\theta(\tau_q)$ are roots of unity. Further, the order of these roots of unity is bounded by a constant depending only on $K$.  

**Proof.** Using Krasner’s lemma, we know that there are only finitely many degree $m$ extensions of $K$. Let $K'$ be the finite extension of $K$ which is the compositum of all the degree $m$ extensions of $K$. By extending scalars to $K'$, we can assume that $\theta(\tau_q)$ is upper triangular. Let $\theta_1, \ldots, \theta_m$ be the diagonal entries. Using equation (1), we deduce that

$$\{\theta_1, \ldots, \theta_m\} = \{\theta_1^q, \ldots, \theta_m^q\}.$$  

From this it follows that the $\theta_i$ are roots of unity (of order dividing $q^m - 1$). Hence the last statement of the lemma follows from the fact that there are only finitely many roots of unity in $K'$.

**Corollary 1.** Let $\theta : G_q \to \text{GL}_m(K)$ be any continuous representation. Assume that the characteristic polynomial of $\theta(\tau_q)$ is not equal to $(x - 1)^m$. Then there exists an integer $N(m,K)$ depending only on $m$ and $K$ such that the reduction modulo $m^N(m,K)$ of any conjugate of $\theta$ into $\text{GL}_m(\mathbb{O})$ is ramified.
Proof. Choose $N(m, K)$ such that if \( \zeta \in K'^\times \) is a root of unity satisfying \( (\zeta - 1)^m \equiv 0 \pmod{mN(m, K)} \), then \( \zeta = 1 \) for \( K' \) as in the proof of Lemma 1. Then the corollary follows by considering reductions of characteristic polynomials.

\[ \square \]

**Corollary 2.** In a continuous, semisimple representation of \( \rho : G_L \to GL_m(K) \), the set of primes \( q \) for which \( \rho(\tau_q) \) is not unipotent is finite.

\[ \square \]

**Corollary 3.** Any continuous, semisimple abelian representation of \( G_L \to GL_m(K) \) is finitely ramified.

\[ \square \]

### 2.4 The \( GL_2 \) case

At this point, for the sake of exposition, we briefly indicate the proof of Theorem 1 when \( m = 2 \) and \( \rho(G_L) \) is open in \( GL_2(K) \) with determinant \( \varepsilon \) the \( p \)-adic cyclotomic character. (Note that in the case when the Lie algebra of \( \rho(G_L) \) is abelian the ramification set is finite by Corollary 3.)

Consider \( S_{\rho, n} \) for \( n > N(2, K) \), and let \( q \in S_{\rho, n} \). Let \( \tilde{\rho}_q \) be any lift of \( \rho_n|_{D_q} \) to \( GL_2(K) \) which is ramified at \( q \). By the above considerations, it follows that \( \tilde{\rho}_q(\tau_q) \) is unipotent, which we can assume to be upper triangular. Since \( \tilde{\rho}_q(\sigma_q) \) normalises \( \tilde{\rho}_q(\tau_q) \), we can assume that

- \( \tilde{\rho}_q(\tau_q) \) is of the form \( \left( \begin{array}{cc} 1 & * \\ 0 & 1 \end{array} \right) \) and \( \tilde{\rho}_q(\tau_q) \) is nontrivial,
- \( \tilde{\rho}_q(\sigma_q) \) is of the form \( \left( \begin{array}{cc} \alpha & 0 \\ 0 & \beta \end{array} \right) \).

Observe that \( \alpha \neq \beta \) because of relation (1). Thus we can further assume by conjugating by an element of the form \( \left( \begin{array}{cc} 1 & 1 \\ 0 & y \end{array} \right) \in GL_2(K) \) that \( \tilde{\rho}_q(\sigma_q) \) is of the form \( \left( \begin{array}{cc} \alpha & 0 \\ 0 & \beta \end{array} \right) \). Then we see from equation (1) that \( \alpha \beta^{-1} = q \).

Consider the invariant functions tr and det defined on the space of conjugacy classes of \( GL_2(0) \) or \( GL_2(0/m^n) \) given by the trace and determinant functions. We see from our work that primes \( q \in S_{\rho, n} \) for \( n > N(2, K) \) are such that the conjugacy classes \( \rho_n(\text{Frob}_{q}) \) satisfy the relation

\[ \text{tr}^2 = (1 + \text{det})^2. \]

From this we conclude, using the fact that the image of \( \rho \) is open in \( GL_2(K) \), Cebotarev density theorem, and the second paragraph of [S1, p. 586], that \( c_{\rho, n} \to 0 \) as \( n \to \infty \).

Proposition 1 follows in this case, and the proof of Theorem 1 is complete in the special case of open image in \( GL_2(K) \) with determinant \( \varepsilon \).

\[ \square \]

### 2.5 The general case

We reduce the general situation to the case when \( \text{im}(\rho) \) is a semisimple \( p \)-adic Lie group.
contained in \( \text{GL}_M(\mathbb{Q}_p) \) for some \( M \). First, by Weil restriction of scalars, we may assume that \( K = \mathbb{Q}_p \) (with possibly a different \( M \)). Let \( G \) be the Zariski closure of the image of \( \rho \). Since \( \rho \) is semisimple, \( G \) is reductive; let \( Z \) be the centre of the connected component of \( G \). Let \( \rho_\alpha : G_1 \to (G/Z)(\mathbb{Q}_p) \) be the corresponding representation. Because of Corollary 2, we see that the ramification set of \( \rho \) and \( \rho_\alpha \) differs by a finite set, and thus we can work with \( \rho_\alpha \). Now embed \( G/Z \) into \( \text{GL}_M/\mathbb{Q}_p \) for some \( M \). Thus we have reduced to the case when \( \text{im}(\rho) \) is a semisimple \( p \)-adic Lie group contained in \( \text{GL}_M(\mathbb{Q}_p) \) for some \( M \).

We look at \( S_{\rho,n} \) for \( n > N(M,\mathbb{Q}_p) \), and we let \( q \in S_{\rho,n} \). Let \( \tilde{\rho}_q \) be any lift of \( \rho_n|_{D_q} \) to \( \text{GL}_M(K) \) which is ramified at \( q \). By Corollary 1, we can assume that \( \tilde{\rho}_q(\tau_q) \) is unipotent (and nontrivial), which we can further assume to be upper triangular.

Consider the canonical filtration of \( \tilde{\rho}_q(\tau_q) \) acting on the vector space \( \mathbb{Q}_p^M \), with the dimension of the corresponding graded components \( m_1,\ldots,m_i \). By conjugating by an element in the Levi, over a finite extension of \( \mathbb{Q}_p \), of the corresponding parabolic subgroup defined by \( \tilde{\rho}_q(\tau_q) \) (of the form \( \text{GL}_{m_1} \times \cdots \times \text{GL}_{m_i} \)), we can assume that \( \tilde{\rho}_q(G_q) \) is upper triangular.

**Lemma 2.** If \( f_q(x) \) is the characteristic polynomial of \( \tilde{\rho}_q(\sigma_q) \), then \( f_q(x) \) and \( f_q(qx) \) have a common root.

**Proof.** Let \( U \) be the subgroup of unipotent upper triangular matrices of \( \text{SL}_M(\mathbb{Q}_p) \), and let

\[
U = U^0 \supset U^1 \supset \cdots \supset 1
\]

be the descending filtration. Let \( i \) be the smallest integer such that \( \tilde{\rho}_q(\tau_q) \notin U^{i+1} \).

By looking at the conjugation action of \( \tilde{\rho}_q(\sigma_q) \) on \( U^i/U^{i+1} \) and using relation (1), it follows that there are two eigenvalues \( \alpha_q, \beta_q \) of \( \tilde{\rho}_q(\sigma_q) \) such that \( \alpha_q \beta_q^{-1} = q \). Hence we have the lemma.

Consider \( \rho' = \rho \oplus \varepsilon : G_1 \to \text{GL}_M(\mathbb{Q}_p) \times \text{GL}_1(\mathbb{Q}_p) \). Let \( G' = G \times \text{GL}_1 \). Choose an integral model for \( \rho' \), that is, \( \rho'(G_1) \subset \text{GL}_M(\mathbb{Z}_p) \times \text{GL}_1(\mathbb{Z}_p) \), induced by the chosen integral model of \( \rho \), and denote by \( \rho'_n \) its reduction mod \( m^n \). We normalise the isomorphism of class field theory so that a uniformiser is sent to the arithmetic Frobenius. (So \( \varepsilon(\text{Frob}_q) = q \).)

Let

\[
(A, b) \in \text{GL}_M(\mathbb{Q}_p) \times \text{GL}_1(\mathbb{Q}_p),
\]

and let \( f(x) \) be the characteristic polynomial of \( A \). Let \( F \) be the invariant polynomial function on \( \text{GL}_M \times \text{GL}_1 \) with \( \mathbb{Z}_p \)-coefficients defined by the resultant of the two polynomials
f(x) and f(bx).

By choosing b different from the ratios of eigenvalues of an element of G, we deduce that no connected component of G' is contained inside the variety \( F = 0 \). Thus we see that \( (F = 0) \cap G' \) is a subvariety of smaller dimension than the dimension of G'.

**Lemma 3.** The image \( \rho'(G_L) \) is an open subgroup of \( G'(Q_p) = G(Q_p) \times GL_1(Q_p) \). \( \square \)

**Proof.** Since \( \text{im}(\rho) \) is a semisimple \( p \)-adic group, we deduce from Chevalley's theorem (see [Bo, Corollary 7.9]) that \( \text{im}(\rho) \) is open in \( G(Q_p) \). From this we further deduce that the commutator subgroup of \( \text{im}(\rho) \) is of finite index in \( \text{im}(\rho) \). Thus the intersection of the fixed fields of the kernel of \( \rho \) and \( \epsilon \) is a finite extension of \( Q \). Certainly \( \text{im}(\epsilon) \) is open in \( Q_p^* \), and hence the lemma follows. \( \blacksquare \)

From the openness of \( \text{im}(\rho') \), we see that

\[
\lim_{n \to \infty} \frac{|\text{im}(\rho'_n)|}{p^{nd}}
\]

is a nonzero positive constant, where \( d \) is the dimension of \( G' \).

On the other hand, using the notation and results of [S1, Section 3], if we denote by \( \widetilde{Y}_n \) the elements \( x \in \text{im}(\rho'_n) \) that satisfy \( F(x) \equiv 0 \pmod{p^n} \), then from the second paragraph of [S1, p. 586] it follows that \( |\widetilde{Y}_n| = O(p^{n(d-\delta)}) \), where \( \delta \) is a positive constant. By Lemma 2, we see that \( \rho'_n(\text{Frob}_q) \in \widetilde{Y}_n \) for \( q \in S_{\rho,n} \). Then applying the Cebotarev density theorem we conclude that

\[
c_{\rho,n} \leq \frac{|\widetilde{Y}_n|}{|\text{im}(\rho'_n)|},
\]

and hence \( c_{\rho,n} \to 0 \) as \( n \to \infty \). This finishes the proof of Proposition 1 and hence of Theorem 1. \( \blacksquare \)

**Remarks.** To prove Theorem 1, instead of defining \( S_{\rho,n} \) the way we did, we could have have worked with the smaller subset consisting of primes that are unramified in \( \rho_n \), but ramified in the \( \rho \) of Theorem 1. In the notation of [S1, p. 586], we would then be working with \( Y_n \) rather than \( \widetilde{Y}_n \). By [S1, Section 3, Theorem 8], we obtain a better estimate \( c_{\rho,n} = O(p^{-n}) \). This may be useful to get more precise quantitative versions of Theorem 1. We have defined \( S_{\rho,n} \) the way we have for its use in [K].

An analog of Theorem 1 is valid for function fields of curves over finite fields of characteristic \( \ell \neq p \), and the same proof works. On the other hand, for function fields of characteristic \( p \), Theorem 1 is false, and in this case there are examples of semisimple \( p \)-adic Galois representations ramified at all places. It is easy to construct such examples using the fact that the Galois group in this case has \( p \)-cohomological dimension less...
than or equal to 1 (see [S3, Chapter II.2, Proposition 3]).

References


Khare: School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400 005, India; shekhar@math.tifr.res.in

Rajan: School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400 005, India; rajan@math.tifr.res.in