Fontaine-Mazur Conjecture and analytic pro-p groups

Supriya Pisolkar

IISER-IISc joint Symposium - Sept. 2021

General context : Understanding Galois groups

General (hard) question: For a number field K, what is $G_K := \mathrm{Gal}(\overline{K}/K)$? How to work out a group structure ?

General context : Understanding Galois groups

General (hard) question: For a number field K, what is $G_K := \mathrm{Gal}(\overline{K}/K)$? How to work out a group structure ?

- **Direct method :** Study its elements and other constituents via group theory and Galois theory

General context : Understanding Galois groups

General (hard) question: For a number field K, what is $G_K := \mathrm{Gal}(\overline{K}/K)$? How to work out a group structure ?

- **Direct method :** Study its elements and other constituents via group theory and Galois theory
- **Indirect method :** Study the action of this group on well-chosen vector spaces via representation theory

General context : Understanding Galois groups

General (hard) question: For a number field K, what is $G_K := \mathrm{Gal}(\overline{K}/K)$? How to work out a group structure ?

- **Direct method :** Study its elements and other constituents via group theory and Galois theory
- **Indirect method :** Study the action of this group on well-chosen vector spaces via representation theory

Mysterious objects - Galois group of an infinite p-extension unramified at the primes above p.

In this talk

The Galois groups of infinite p-extensions unramaified at the prime above p :

In this talk

The Galois groups of infinite p-extensions unramaified at the prime above p :

1. They are studied mainly with the group theoretic techniques (methods which are less known to modern arithmetic geometers).
2. How these group theoretic techniques have contributed in providing evidence to the analogues of F-M conjecture.

In this talk

The Galois groups of infinite p-extensions unramaified at the prime above p :

1. They are studied mainly with the group theoretic techniques (methods which are less known to modern arithmetic geometers).
2. How these group theoretic techniques have contributed in providing evidence to the analogues of F-M conjecture.

Joint work with : R. Abdellatif, J. Lang, M. Rougnant and L. Thomas

Fontaine-Mazur conjecture

K - number field, $G_K := \mathrm{Gal}(\overline{K}/K)$ and p- prime number.

Definition

A p-adic representation ρ of G_K is called geometric if it ramifies only at a finite number of places of K, and if for each place v of K dividing p, the restriction of ρ to G_v is potentially semi-stable in the sense of Fontaine.

Fontaine-Mazur conjecture

K - number field, $G_K := \mathrm{Gal}(\overline{K}/K)$ and p- prime number.

Definition

A p-adic representation ρ of G_K is called geometric if it ramifies only at a finite number of places of K, and if for each place v of K dividing p, the restriction of ρ to G_v is potentially semi-stable in the sense of Fontaine.

A remarkable conjecture of Fontaine and Mazur says.

Conjecture (Fontaine, Mazur)

An irreducible p-adic representation of G_K is geometric if and only if it is isomorphic to a subquotient of an étale cohomology group with coefficients in some Tate twist $Q_p(r)$, $r \in \mathbb{Z}$, of a (projective, smooth) algebraic variety over K.

Fontaine-Mazur conjecture

K - number field, $G_K := \mathrm{Gal}(\overline{K}/K)$ and p- prime number.

Definition

A p-adic representation ρ of G_K is called geometric if it ramifies only at a finite number of places of K, and if for each place v of K dividing p, the restriction of ρ to G_v is potentially semi-stable in the sense of Fontaine.

A remarkable conjecture of Fontaine and Mazur says.

Conjecture (Fontaine, Mazur)

An irreducible p-adic representation of G_K is geometric if and only if it is isomorphic to a subquotient of an étale cohomology group with coefficients in some Tate twist $Q_p(r)$, $r \in \mathbb{Z}$, of a (projective, smooth) algebraic variety over K.

The case $n = 1$ follows by class field theory and the case $K = \mathbb{Q}$ and $n = 2$ follows by the methods of Wiles, Taylor-Wiles and Skinner-Wiles.

The theory comes in two flavours :
(1)(Wild case) primes above p are in S (2) (Tame case) primes above p are not in S.

The theory comes in two flavours :
(1)(Wild case) primes above p are in S (2) (Tame case) primes above p are not in S.

Conjecture (Tame F-M conjecture)

If $\rho : G(\overline{K}/K) \to GL_n(\mathbb{Q}_p)$ is a p-adic representation unramified at outside S where

- *S contains no primes above p*
- *S is finite*

The the image of ρ is finite.

The theory comes in two flavours :
(1)(Wild case) primes above p are in S (2) (Tame case) primes above p are not in S.

Conjecture (Tame F-M conjecture)

If $\rho : G(\overline{K}/K) \to GL_n(\mathbb{Q}_p)$ is a p-adic representation unramified at outside S where

- *S contains no primes above p*
- *S is finite*

The the image of ρ is finite.

This is equivalent to saying that there does not exist $\rho : G(\overline{K}/K) \to GL_n(\mathbb{Q}_p)$ with infinite image.

Theorem (Lazard)

A topological group has a structure of a p-adic analytic group is and only if it contains an (open) uniform pro-p subgroup.

Thus the Fontaine-Mazur conjecture for $S = \phi$ is equivalent to :

Conjecture (F-M conjecture - Uniform version)

There does not exist a number field and an infinite everywhere unramified Galois pro-p extension L such that $G(L/K)$ is uniform.

Pro-p groups

Pro-p groups

G- profinite group, the Frattini subgroup $\Phi(G) := \bigcap M$, where the intersection runs over all maximal proper open subgroups.

Pro-p groups

G- profinite group, the Frattini subgroup $\Phi(G) := \bigcap M$, where the intersection runs over all maximal proper open subgroups.

- A pro-p-group G is finitely generated if and only if, its Frattini subgroup $\Phi(G)$ is open in G.
- The *lower p-series* of a pro-p-group G is the series $(P_i(G))_{i\geq 1}$ of topologically characteristic subgroups of G defined as follows:
  1. $P_1(G) := G$;
  2. $\forall\ i \geq 1,\ P_{i+1}(G) := \overline{P_i(G)^p[P_i(G), G]}$.
- For any pro-p-group G, $\Phi(G) = P_2(G) (= \overline{G^p[G, G]})$.
- For any finitely generated pro-p-group G,

$$d(G) := \dim_{\mathbb{F}_p} G/\Phi(G)\ .$$

It is also equal to the minimal cardinality of a topological generating set for G, which also matches with the dimension as p-adic analytic group, provided such a structure exists.

Uniform (Powerful) pro-p groups

Definition

A p-group G is *powerful* when:

- either p is odd, and G/G^p is an abelian group;
- or $p = 2$, and G/G^4 is an abelian group.

Definition

A *uniform* group G is a powerful, finitely generated pro-p-group G such that, for all $i \geq 1$, we have $[P_i(G) : P_{i+1}(G)] = [G : P_2(G)]$.

$SL_n^1(\mathbb{Z}_p) := \ker\left(SL_n(\mathbb{Z}_p) \twoheadrightarrow SL_n(\mathbb{Z}/p\mathbb{Z})\right)$ (for $p = 2$ or *odd*) is a uniform group of dimension $n^2 - 1$.

N. Boston's results

N. Boston's results

N. Boston gave the first evidence to the truth of the uniform version of F-M C . Instead of representation theoretic techniques, he developed purely group theoretic methods related to the powerful pro-p groups and uniform pro-p groups these results.

N. Boston's results

N. Boston gave the first evidence to the truth of the uniform version of F-M C . Instead of representation theoretic techniques, he developed purely group theoretic methods related to the powerful pro-p groups and uniform pro-p groups these results.

Theorem (N. Boston, 1992)

Let K be a normal extension of prime degree $\ell \neq p$ of a number field F such that $p \nmid h(F)$, the class number of F. Then there is no infinite everywhere unramified Galois pro-p extension L of K such that L is Galois over F and $G(L/K)$ is uniform .

Boston generalised this result to the case where $[K : F]$ is a cyclic extension of degree n where $(n, p) = 1$. The main ingredient of the group theoretic methods to prove these results is the cyclic action of σ on the Galois group $G(L/K)$, where σ is a generator of the Galois group $G(K/F)$.

Idea of Boston's proof

Suppose there exists a uniform group $G(L/K)$ with the conditions as in the hypothesis. By Schur-Zassenhaus theorem there exists a split exact sequence,

$$1 \to G(L/K) \to G(L/F) \to G(K/F) \to 1$$

There exists a $\sigma \in G(L/F)$ mapping onto a generator of $G(K/F)$, inducing conjugation action on $G(L/K)$. Further we derive that σ can not act fixed point free on all quotients G/P_i. Pick minimal i so that there is a $\tau \in G/P_i$ such that $\sigma \cdot \tau = \tau$. By using the isomorphism $P_{i-1}/P_i \to P_{i-2}/P_{i-1}$ we will get a a fixed point in $G/P_2 = G/\Phi(G)$ which is a $\mathbb{F}_p$ vector space.

Idea of Boston's proof

Suppose there exists a uniform group $G(L/K)$ with the conditions as in the hypothesis. By Schur-Zassenhaus theorem there exists a split exact sequence,

$$1 \to G(L/K) \to G(L/F) \to G(K/F) \to 1$$

There exists a $\sigma \in G(L/F)$ mapping onto a generator of $G(K/F)$, inducing conjugation action on $G(L/K)$. Further we derive that σ can not act fixed point free on all quotients G/P_i. Pick minimal i so that there is a $\tau \in G/P_i$ such that $\sigma \cdot \tau = \tau$. By using the isomorphism $P_{i-1}/P_i \to P_{i-2}/P_{i-1}$ we will get a a fixed point in $G/P_2 = G/\Phi(G)$ which is a $\mathbb{F}_p$ vector space.
Now σ is of order co-prime to p so by Maschke's theorem one can deduce that there exists a cyclic p extension M (unramified) inside L. One can deduce from here that there exists a degree p unramified extension of F inside M, which contradicts the fact that $p \nmid h(F)$.

Boston's method works when there are no non-trivial fixed points for the action of σ on $G(L/K)$. Hajir and Maire attempted to extend Boston's strategy to the case of (tamely) ramified L/K. The challenge was to handle the fixed points introduced by ramification and as a consequence, the constraints posed on the arithmetic of L/K.

Conjecture (Tame F-M Conjecture- Uniform version)

Suppose K is a number field and Γ is a uniform pro-p group of dimension $d > 2$. Then there does not exists a finitely tamely ramified Galois extension L/K with Galois group $\Gamma = G(L/K)$.

Boston's method works when there are no non-trivial fixed points for the action of σ on $G(L/K)$. Hajir and Maire attempted to extend Boston's strategy to the case of (tamely) ramified L/K. The challenge was to handle the fixed points introduced by ramification and as a consequence, the constraints posed on the arithmetic of L/K.

Conjecture (Tame F-M Conjecture- Uniform version)

Suppose K is a number field and Γ is a uniform pro-p group of dimension $d > 2$. Then there does not exists a finitely tamely ramified Galois extension L/K with Galois group $\Gamma = G(L/K)$.

Let $(S, p) = 1$, T be a finite set such that $S \cap T = \phi$, K_S^T - maximal pro-p extension of K unramified outside S, in which places in T split completely.

Let $(S, p) = 1$, T be a finite set such that $S \cap T = \phi$, K_S^T - maximal pro-p extension of K unramified outside S, in which places in T split completely. One can show that $G_S^T := G(K_S^T/K)$ is the p-Sylow subgroup of the T-ray class group of K mod S.

Let $(S, p) = 1$, T be a finite set such that $S \cap T = \phi$, K_S^T - maximal pro-p extension of K unramified outside S, in which places in T split completely. One can show that $G_S^T := G(K_S^T/K)$ is the p-Sylow subgroup of the T-ray class group of K mod S.

K- number field admitting a non-trivial automorphism σ of prime order ℓ dividing $p-1$, and $k = K^\sigma$ is the fixed field of $\Delta =< \sigma >$. We will assume that the sets S and T described above are stable under the action of σ. Thus, the extension K_S^T/k is Galois and σ acts on G_S^T.

Let $(S, p) = 1$, T be a finite set such that $S \cap T = \phi$, K_S^T - maximal pro-p extension of K unramified outside S, in which places in T split completely. One can show that $G_S^T := G(K_S^T/K)$ is the p-Sylow subgroup of the T-ray class group of K mod S.

K- number field admitting a non-trivial automorphism σ of prime order ℓ dividing $p-1$, and $k = K^\sigma$ is the fixed field of $\Delta =< \sigma >$. We will assume that the sets S and T described above are stable under the action of σ. Thus, the extension K_S^T/k is Galois and σ acts on G_S^T.

Definition : Let $\rho : G_S^T \to GL_n(\mathbb{Q}_p)$, and L - subfield of K_S^T fixed by $ker(\rho)$ so that the image of ρ (say Γ) is naturally identified with $G(L/K)$. We say that ρ or Γ is σ-uniform if we have (i) $\Gamma = G(L/K)$ is uniform; and (ii) L/k is Galois, i.e. the action of σ on G_S^T induces an action on Γ.

Theorem (Hajir-Maire- 2018)

K/k - quadratic extension, an odd prime $p \nmid Cl(k)$. Let $\Gamma = SL_2^1(\mathbb{Z}_p)$. Suppose, for all finite sets Σ of places of k with $(\Sigma, p) = 1$, there exist infinitely many disjoint finite sets S and T of primes of K, with $(S, p) = 1$and $|S|$ arbitrarily large such that,

1. *$G_S^T/\Phi(G_S^T)$ has S independent fixed points under the action of σ*
2. *there is no continuous representation $\rho : G_S^T \twoheadrightarrow \Gamma$.*

Theorem (Hajir-Maire- 2018)

K/k - quadratic extension, an odd prime $p \nmid Cl(k)$. Let $\Gamma = SL_2^1(\mathbb{Z}_p)$. Suppose, for all finite sets Σ of places of k with $(\Sigma, p) = 1$, there exist infinitely many disjoint finite sets S and T of primes of K, with $(S, p) = 1$ and $|S|$ arbitrarily large such that,

1. *$G_S^T/\Phi(G_S^T)$ has S independent fixed points under the action of σ*
2. *there is no continuous representation $\rho : G_S^T \twoheadrightarrow \Gamma$.*

Key ingredient : Γ - uniform group with $\sigma \in Aut(\Gamma)$ of order $\ell \mid p-1$, and Γ_σ is the normal closure of fixed points of σ. Then the action of σ is said to be 'fixed point mixing modulo Frattini' if σ acts nontrivially on $\Gamma_\sigma/\Phi(\Gamma_\sigma)$.

R. Ramakrishna's counter example

Fontaine and Mazur asked whether the condition 'S is a finite set' in the Tame F-M conjecture holds automatically for every semi-simple n-dimensional p-adic representation.

R. Ramakrishna's counter example

Fontaine and Mazur asked whether the condition 'S is a finite set' in the Tame F-M conjecture holds automatically for every semi-simple n-dimensional p-adic representation.

For $n = 2$, Ramakrishna answered this question negatively. He also constructed, under GRH, an irreducible 2-dimensional representation ramified at infinitely many primes but not at p .

Bi-quadratic case: Work in progress with R. Abdellatif

Theorem (Boston)

Let K be a normal extension of prime degree $\ell \neq p$ of a number field F such that $p \nmid h(F)$, the class number of F. Then there is no infinite everywhere unramified Galois pro-p extension L of K such that L is Galois over F and $G(L/K)$ is uniform .

Bi-quadratic case: Work in progress with R. Abdellatif

Theorem (Boston)

Let K be a normal extension of prime degree $\ell \neq p$ of a number field F such that $p \nmid h(F)$, the class number of F. Then there is no infinite everywhere unramified Galois pro-p extension L of K such that L is Galois over F and $G(L/K)$ is uniform .

Example(D. Buell) : $K = \mathbb{Q}(\sqrt{-104}, \sqrt{229})$ with $p = 3$. Then $3 \mid h(K)$. Let G be the Galois group of a maximal everywhere unramified pro-p extension of K. We have observed the following by SAGE computations:

- $3|h(K)$
- $G/\Phi(G) = G^{ab} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
- $d(G) = dim_{\mathbb{F}_3}(H^1(G, \mathbb{F}_3)) = 3$ and $r(G) = dim_{\mathbb{F}_3}(H^2(G, \mathbb{F}_3)) = 3 or 4$.

Bi-quadratic case: Work in progress with R. Abdellatif

Theorem (Boston)

Let K be a normal extension of prime degree $\ell \neq p$ of a number field F such that $p \nmid h(F)$, the class number of F. Then there is no infinite everywhere unramified Galois pro-p extension L of K such that L is Galois over F and $G(L/K)$ is uniform .

Example(D. Buell) : $K = \mathbb{Q}(\sqrt{-104}, \sqrt{229})$ with $p = 3$. Then $3 \mid h(K)$. Let G be the Galois group of a maximal everywhere unramified pro-p extension of K. We have observed the following by SAGE computations:

- $3|h(K)$
- $G/\Phi(G) = G^{ab} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
- $d(G) = dim_{\mathbb{F}_3}(H^1(G, \mathbb{F}_3)) = 3$ and $r(G) = dim_{\mathbb{F}_3}(H^2(G, \mathbb{F}_3)) = 3 or 4$.

Question: G have an infinite p-adic analytic pro-p quotient?

Question: G have an infinite p-adic analytic pro-p quotient?

Lemma

Suppose G is any infinite, finitely generated pro-p group such that

1. *the Bockestein map $H^1(G, \mathbb{Z}/p\mathbb{Z}) \to H^2(G, \mathbb{Z}/p\mathbb{Z})$ is an isomorphism*
2. *the cup-product map $H^1(G, \mathbb{Z}/p\mathbb{Z}) \wedge H^1(G, \mathbb{Z}/p\mathbb{Z}) \to H^2(G, \mathbb{Z}/p\mathbb{Z})$ is an isomorphism*

Then $G \cong SL_2^1(\mathbb{Z}_p) := Ker(SL_2(\mathbb{Z}_p) \to SL_2(\mathbb{Z}/p\mathbb{Z}))$.

Note that $SL_2^1(\mathbb{Z}_P)$ is a uniform pro-p group. Thus if the above two conditions are satisfied by $Gal(L/K)$ then we could conclude that Boston's result fails in this case.

Bockestein map is an isomorphism?

By using the long exact sequence of cohomology groups induced by the short exact sequence

$$0 \to \mathbb{Z}/3\mathbb{Z} \xrightarrow{\cdot 3} \mathbb{Z}/3^2\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \to 0$$

and by using the fact that $G^{ab} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ we have

Lemma

For $p = 3$ and K and L be as before, then the Bockstein map is injective.

If we could show that
$d(G) = dim_{\mathbb{F}_p} H^1(G, \mathbb{Z}/3\mathbb{Z}) = dim_{\mathbb{F}_p} H^2(G, \mathbb{Z}/3\mathbb{Z}) = 3$ then we are done.

Theorem

For $p = 3$ and $G = Gal(L/K)$, the cup product map

$$H^1(G, \mathbb{Z}/p\mathbb{Z}) \wedge H^1(G, \mathbb{Z}/p\mathbb{Z}) \to H^2(G, \mathbb{Z}/p\mathbb{Z})$$

is injective.

The proof of this heavily depends on the SAGE computations. As a corollary to this theorem we derive that G is a powerful pro-p group.

Thank You