LINKING NUMBERS AND THE TAME FONTAINE-MAZUR CONJECTURE

JOHN LABUTE

Abstract. Let p be an odd prime, let S be a finite set of primes $q \equiv 1 \bmod p$ but $q \not\equiv 1 \bmod p^2$ and let G_S be the Galois group of the maximal p-extension of $\mathbb{Q}$ unramified outside of S. If ρ is a continuous homomorphism of G_S into $\mathrm{GL}_2(\mathbb{Z}_p)$ then under certain conditions on the linking numbers of S we show that $\rho = 1$ if $\overline{\rho} = 1$. We also show that $\overline{\rho} = 1$ if ρ can be put in triangular form mod p^3.

To Helmut Koch on his 80th birthday

1. Statement of Results

Let p be a rational prime. Let K be a number field, let S be a finite set of primes of K with residual characteristics $\neq p$ and let $\Gamma_{S,K}$ be the Galois group of the maximal (algebraic) extension of K unramified outside of S. The Tame Fontaine-Mazur Conjecture (cf. [1], Conj. 5a) states that every continuous homomorphism

$$\rho : \Gamma_{S,K} \to \mathrm{GL}_n(\mathbb{Z}_p)$$

has a finite image. If $\overline{\rho}$ is the reduction of ρ mod p then $\overline{\rho}$ is trivial if and only if the image of ρ is contained in the standard subgroup

$$\mathrm{GL}_n^{(1)}(\mathbb{Z}_p) = \{X \in \mathrm{GL}_n(\mathbb{Z}_p) \mid X \equiv 1 \bmod p\}$$

which is a pro-p-group. Hence, if $\overline{\rho} = 1$, the homomorphism ρ factors through $G_{S,K}$, the maximal pro-p-quotient of $\Gamma_{S,K}$. Since $\mathrm{GL}_n^{(1)}(\mathbb{Z}_p)$ is torsion free, this shows that when $\overline{\rho} = 1$ the Tame Fontaine-Mazur Conjecture is equivalent to the following conjecture.

Conjecture 1.1. *If $\rho : G_{S,K} \to \mathrm{GL}_n^{(1)}(\mathbb{Z}_p)$ is a continuous homomorphism then $\rho = 1$.*

Conversely, the truth of Conjecture 1.1 for any number field K implies the Fontaine-Mazur Conjecture. In this paper we will prove Conjecture 1.1 when $K = \mathbb{Q}$ for certain sets S.

We now let $K = \mathbb{Q}$ and $G_S = G_{S,\mathbb{Q}}$. To prove Conjecture 1.1 we can assume that the primes in S are congruent to 1 mod p since these are the only primes different from p that can ramify in a p-extension of $\mathbb{Q}$. We will also assume that the primes in S are not congruent to 1 mod p^2, which is equivalent to $G_S/[G_S, G_S]$ being elementary. In this case we will show that Conjecture 1.1 follows from a Lie theoretic analogue of it when p is odd. We therefore assume that $p \neq 2$ for the rest of the paper.

Date: May 15, 2013.

1991 *Mathematics Subject Classification.* 11R34, 20E15, 12G10, 20F05, 20F14, 20F40.

†Research supported in part by an NSERC Discovery Grant.

To formulate this analogue let $S = \{q_1, \dots, q_d\}$ and let $\mathfrak{l}_S$ be the finitely presented Lie algebra over $\mathbb{F}_p$ generated by $\xi_1, \dots, \xi_d$ with relators $\sigma_1, \dots, \sigma_d$ where

$$\sigma_i = c_i \xi_i + \sum_{j \neq i} \ell_{ij}[\xi_i, \xi_j]$$

with $c_i = (q_i - 1)/p \bmod p$ and the linking number ℓ_{ij} of (q_i, q_j) defined by $q_i \equiv g_j^{-\ell_{ij}}$ mod q_j with g_j a primitive root mod q_j. We call $\mathfrak{l}_S$ the linking algebra of S. Up to isomorphism, it is independent of the choice of primitive roots.

Theorem 1.2. *There exists a mapping*

$$\ell : \mathrm{Hom}_{cont}(G_S, \mathrm{GL}_n^{(1)}(\mathbb{Z}_p)) \to \mathrm{Hom}(\mathfrak{l}_S, gl_n(\mathbb{F}_p))$$

such that $\rho = 1 \iff \ell(\rho) = 0$.

Corollary 1.3. *If the cup-product* $H^1(G_S, \mathbb{F}_p) \times H^1(G_S, \mathbb{F}_p) \to H^2(G_S, \mathbb{F}_p)$ *is trivial then Conjecture 1.1 is true for* G_S.

Definition 1.4 (Property $FM(n)$)**.** A Lie algebra $\mathfrak{g}$ over a field F is said to have Property $FM(n)$ if every n-dimensional representation of $\mathfrak{g}$ is trivial.

Theorem 1.5. *If* $\mathfrak{l}_S$ *has Property* $FM(k)$ *then Conjecture 1.1 is true for* $n = k$.

If $|S| \leq 2$ then $\mathfrak{l}_S$ has Property $FM(n)$ for all n since $\mathfrak{l}_S = 0$ in this case. However $\mathfrak{l}_S$ may not have Property $FM(2)$ if $|S| \geq 3$; for example, if $p = 3$, $S = \{7, 31, 229\}$ or if $p = 5$ and $S = \{11, 31, 1021\}$. However, the number of such S is relatively small; for example, if $p = 7$ and the primes in S are at most $10,000$, the set S fails to have Property $FM(2)$ approximately $.2\%$ of the time. The following theorem gives necessary and sufficient conditions for Property $FM(n)$ to hold when $|S| = 3$.

Theorem 1.6. *Let* $m_{ij} = -\ell_{ij}/c_i$. *If* $|S| = 3$ *and* $n < p$ *then Property* $FM(n)$ *holds if and only if one of the following conditions holds:*
(a) $m_{ij} = 0$ *for some* i, j;
(b) $m_{ij} \neq 0$ *for all* i, j *and* $m_{ik} = m_{jk}$ *for some* i, j, k *with* $i \neq j$;
(c) $m_{ij} \neq 0$ *for all* i, j *and* $(m_{ik} - m_{jk})(m_{ki}m_{ij} - m_{kj}m_{ji}) \neq 0$ *for some* i, j, k.
These conditions are independent of the choice of primitive roots.

Theorem 1.7. *If* $|S| = 3$ *and* $n < p$ *then* $\mathfrak{l}_S$ *fails to have Property* $FM(n)$ *if and only if* $\ell_{ij} \neq 0$ *for all* i, j *and* $\ell_{13}/c_1 = -\ell_{23}/c_2,\ \ell_{21}/c_2 = -\ell_{31}/c_3,\ \ell_{12}/c_1 = -\ell_{32}/c_3$.

Theorem 1.8. *Let* $\rho : G_S \to \mathrm{GL}_2(\mathbb{Z}_p)$ *be a continuous homomorphism. Then* $\overline{\rho} = 1$ *if* ρ *can be brought to triangular form mod* p^3.

The pro-p-groups G_S are very mysterious. They are all fab groups, i.e., subgroups of finite index have finite abelianizations, and for $|S| \geq 4$ they are not p-adic analytic. So far no one has given a purely algebraic construction of such a pro-p-group. We call a pro-p-group G a Fontaine-Mazur group if every continuous homomorphism of G into $\mathrm{GL}_n(\mathbb{Z}_p)$ is finite. Again, no purely algebraic construction of such a group exists. In this direction we have the following result.

Theorem 1.9. *Let G be the pro-p-group with generators $x_1, \dots, x_{2m}$ and relations*

$$x_1^{pc_1}[x_1, x_2] = 1,\ x_2^{pc_2}[x_2, x_3] = 1, \dots,\ x_{2m-1}^{pc_{2m-1}}[x_{2m-1,2m}] = 1,\ x_{2m}^{pc_{2m}}[x_{2m}, x_1] = 1$$

with $c_i \not\equiv 0$ mod p and $p > 2$, $m \geq 2$. Then every continuous homomorphism of G into $\mathrm{GL}_n^{(1)}(\mathbb{Z}_p)$ is trivial if $n < p$.

2. Mild pro-p-groups

Let G be a pro-p-group. The descending central series of G is the sequence of subgroups G_n defined for $n \geq 1$ by

$$G_1 = G, \quad G_{n+1} = G_n^p[G, G_n]$$

where $G_n^p[G, G_n]$ is the closed subgroup of G generated by p-th powers of elements of G_n and commutators of the form $[h, k] = h^{-1}k^{-1}hk$ with $h \in G$ and $k \in G_n$. The graded abelian group

$$\mathrm{gr}(G) = \oplus_{n\geq 1}\mathrm{gr}_n(G) = \oplus_{n\geq 1} G_n/G_{n+1}$$

is a graded vector space over $\mathbb{F}_p$ where $\mathrm{gr}_n(G)$ is denoted additively. We let

$$\iota_n : G_n \to \mathrm{gr}_n(G)$$

be the quotient map. Since $p \neq 2$, the graded vector space $\mathrm{gr}(G)$ has the structure of a graded Lie algebra over $\mathbb{F}_p[\pi]$ where

$$\pi\, \iota_n(x) = \iota_{n+1}(x^p), \quad [\iota_n(x), \iota_m(y)] = \iota_{n+m}([x, y]).$$

Let $G = F/R$ where F is the free pro-p-group on $x_1, \dots, x_d$ and $R = (r_1, \dots, r_m)$ is the closed normal subgroup of F generated by $r_1, \dots, r_m$ with $r_i \in F_2$. If

$$r_k \equiv \prod_{i\geq 1} x_i^{pa_j} \prod_{i<j} [x_i, x_j]^{a_{ijk}} \mod F_3$$

and we let $\xi_i = \iota_1(x_1)$, $\rho_k = \iota_2(r_k)$ in $L = \mathrm{gr}(F)$ then L is the free Lie algebra over $\mathbb{F}_p[\pi]$ on $\xi_1, \dots, \xi_d$ and

$$\rho_k = \sum_{i\geq 1} a_i \pi \xi_i + \sum_{i<j} a_{ijk}[\xi_i, \xi_j].$$

Let $\mathfrak{r}$ be the ideal of L generated by $\rho_1, \dots \rho_m$, let $\mathfrak{g} = L/\mathfrak{r}$ and let U be the enveloping algebra of $\mathfrak{g}$. Then $\mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]$ is a U-module via the adjoint representation. The sequence $\rho_1, \dots, \rho_m$ is said to be **strongly free** if (a) $\mathfrak{g}$ is a torsion-free $\mathbb{F}_p[\pi]$-module and (b) $\mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]$ is a free U-module on the images of $\rho_1, \dots, \rho_m$ in which case we say that the presentation is strongly free.

Theorem 2.1 ([3], Theorem 1.1)**.** *If $G = F/R$ is strongly free then $\mathfrak{r}$ is the kernel of the canonical surjection $\mathrm{gr}(F) \to \mathrm{gr}(G)$ so that $\mathrm{gr}(G) = L/\mathfrak{r}$.*

A finitely presented pro-p-group G is said to be **mild** if it has a strongly free presentation.

Let $A = \mathbb{Z}_p[[G]]$ be the completed algebra of G and let $I = \mathrm{Ker}(A \to \mathbb{F}_p)$ be the augmentation ideal of $\mathbb{Z}_p[[G]]$. Then

$$\mathrm{gr}(A) = \oplus_{n\geq 1} I^n/I^{n+1}$$

is a graded algebra over $\mathbb{F}_p[\pi]$ where π can be identified with the image of p in I/I^2. The canonical injection of G into A sends G_n into $1 + I^n$ and gives rise to a canonical Lie algebra homomorphism of $\mathrm{gr}(G)$ into $\mathrm{gr}(A)$ which is injective if and only if $G_n = G \cap (1 + I^n)$.

Theorem 2.2 ([3], Theorem 1.1)**.** *If G is mild the canonical map $\mathrm{gr}(G) \to \mathrm{gr}(A)$ is injective and $\mathrm{gr}(A)$ is the enveloping algebra of $\mathrm{gr}(G)$. Moreover, $R/[R,R]$ is a free A-module which implies that $\mathrm{cd}(G) \leq 2$.*

We now give a criterion for the mildness of $G = G_S$ when $p \neq 2$ and $p \notin S$. The group G_S has a presentation $F(x_1, \ldots, x_d)/(r_1, \ldots, r_d)$ where x_i is a lifting of a generator of an inertia group at q_i and

$$r_i = x_i^{pc_i} \prod_{j \neq i} [x_i, x_j]^{\ell_{ij}} \mod F_3$$

which is due to Helmut Koch ([2], Example 11.11). Using the transpose of the inverse of the transgression isomorphism

$$\mathrm{tg} : H^1(R, \mathbb{F}_p)^F = (R/R^p[R,F])^* \longrightarrow H^2(G, \mathbb{F}_p),$$

the relator r_i defines a linear form ϕ_i on $H^2(G, \mathbb{F}_p))$ such that, if $\chi_1, \ldots, \chi_d$ is the basis of $H^1(F, \mathbb{F}_p) = (F/F^p[F,F])^*$ with $\chi_i(x_j) = \delta_{ij}$, we have $\phi_i(\chi_i \cup \chi_j) = -\ell_{ij}$ if $i < j$; cf.[2], Theorem 7.23.

The set S is said to be a **circular set** of primes if there is an ordering $q_1, \ldots, q_d$ of the set S such that

(a) $\ell_{i,i+1} \neq 0$ for $1 \leq i < d$ and $\ell_{d1} \neq 0$,
(b) $\ell_{ij} = 0$ if i, j are odd,
(c) $\ell_{12}\ell_{23} \cdots \ell_{d-1,d}\ell_{d1} \neq \ell_{1m}\ell_{m,m-1} \cdots \ell_{32}\ell_{21}$.

Theorem 2.3. *If S is a circular set of primes then G_S is mild.*

Theorem 2.4. *The set S can be extended to a set $S \cup q$ where $q \equiv 1$ mod p, $q \not\equiv 1$ mod p^2 in such a way that the pairs (q, q_i), (q_i, q) with non-zero linking numbers can be arbitrarily prescribed.*

Corollary 2.5. *The set S can always extended to a set S' with $G_{S'}$ mild.*

See Labute ([3], Theorem 1.1) for the proof of Theorem 2.3 and ([3], Proposition 6.1) for the proof of Theorem 2.4. The proof of Proposition 6.1 in [3] yields the sharper form stated here.

Theorem 2.6. *There exists a finite set $S' \supseteqq S$ consisting of primes $q \equiv 1$ mod p, $q \not\equiv 1$ mod p^2 such that $G_{S'}$ is mild and, if $n < p$, the Lie algebra $\mathfrak{l}_{S'}$ has Property(FM(n)) if $\mathfrak{l}_S$ does.*

3. Proof of Theorem 1.2

Let G be a pro-p-group with $G/[G,G] \cong (\mathbb{Z}/p\mathbb{Z})^d$ and let $\rho : G \to \mathrm{GL}_n^{(1)}(\mathbb{Z}_p)$ be a continuous homomorphism. Let

$$\mathrm{GL}_n^{(k)}(\mathbb{Z}_p) = \{X \in \mathrm{GL}_n(\mathbb{Z}_p) \mid X \equiv 1 \bmod p^k\}.$$

Lemma 3.1. *Let $X = 1 + p^i A \in \mathrm{GL}_n^{(i)}(\mathbb{Z}_p)$, $Y = 1 + p^j B \in \mathrm{GL}_n^{(j)}(\mathbb{Z}_p)$ then*
$[X, Y] = 1 + p^{i+j}[A, B] \bmod p^{i+j+1}$, $X^p = 1 + p^{i+1} A \bmod p^{i+2}$, *where* $[A, B] = AB - BA$.

Lemma 3.2. *If $\rho(G) \neq 1$ then $\rho(G) \not\subseteq \mathrm{GL}_n^{(2)}(\mathbb{Z}_p)$.*

Proof. Let $H = \rho(G)$ and let $k \geq 1$ be largest with $H \subseteq \mathrm{GL}_n^{(k)}(\mathbb{Z}_p)$. Let $h_1, \dots h_d$ be a generating set for H and let $h_i = I + p^k N_i$. Then $[h_i, h_j] \in \mathrm{GL}_n^{(2k)}(\mathbb{Z}_p)$ which implies that $[H, H] \subseteq \mathrm{GL}_n^{(2k)}(\mathbb{Z}_p)$. By assumption, there exists i such that $N_i \not\equiv 0 \mod p$. But

$$h_i^p = (1 + p^k N_i)^p \equiv 1 + p^{k+1} N_i \mod p^{k+2}.$$

Since $N_i \not\equiv 0$ modulo p we have $h_i^p \in [H, H]$ only if $k + 1 \geq 2k$ which implies that $k = 1$. □

Let $G = G_S$. Then G_S has the presentation $F(x_1, \dots, x_d)/(r_1, \dots, r_d)$ where

$$r_i = x_i^{pc_i} \prod_{j \neq i} [x_i, x_j]^{\ell_{ij}} \mod F_3.$$

Let $\rho(x_i) = 1 + pA_i$. Then modulo p^3 we have

$$1 = \rho(r_i) = 1 + p^2(c_i A_i + \sum_{j \neq i} \ell_{ij} [A_i, A_j]).$$

Hence, if $\overline{A}_i$ is the image of A_i in $gl_n(\mathbb{F}_p)$, we have

$$c_i \overline{A}_i + \sum_{j \neq i} \ell_{ij} [\overline{A}_i, \overline{A}_j] = 0.$$

Thus $\ell(\rho)(\xi_i) = \overline{A}_i$ defines a Lie algebra homomorphism $\ell(\rho) : \mathfrak{l}_S \to sl_n(\mathbb{F}_p)$. If $\rho = 1$ then $A_i = 0$ for all i which implies $\ell(\rho) = 0$. Conversely, if $\rho \neq 1$ then by Lemma 3.2 we have $\overline{A}_i \neq 0$ for some i which implies $\ell(\rho) \neq 0$.

4. Proof of Theorem 1.8

Without loss of generality, we can assume that G_S is mild. Let $H = \rho(G_S)$ and assume that $\overline{H} = \overline{\rho}(G_S) \neq 1$. Note that H is a subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ since $G_S/[G_S, G_S]$ is finite. After a change of basis, we can assume that the matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in H$ satisfy $p^3 | c$ and that $\overline{H}$ is generated by the image of

$$C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Let $h_1, \dots, h_d$ be a generating set for H with $h_1, \dots, h_{d-1} \in \mathrm{SL}_n^{(1)}(\mathbb{Z}_p)$ and $h_d \equiv C \mod p$. We have

$$h_i - 1 = pA_i = p \begin{bmatrix} a_i & b_i \\ c_i & d_i \end{bmatrix} \text{ for } i < d \text{ and } h_d - 1 = \begin{bmatrix} p\, a_d & 1 + p\, e \\ p\, c_d & p\, f \end{bmatrix}.$$

We also have $d > 1$ since otherwise H is infinite cyclic which is impossible since $H/[H, H]$ is finite.

Lemma 4.1. *Let $X, Y \in \mathrm{GL}_2(\mathbb{Z}_p)$ with $X = 1 + pA = 1 + p \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and with $Y \equiv C \mod p$. Then*

$$[X, Y] \equiv 1 + p \begin{bmatrix} -c & a - d - c \\ 0 & c \end{bmatrix} \mod p^2.$$

Proof. Let $N = Y - 1$. Then, working mod p^2, we have

$$\begin{aligned}[X,Y] &\equiv (1+pA)^{-1}(1+N)^{-1}(1+pA)(1+N)\\ &\equiv (1-pA)(1-N+N^2-N^3)(1+pA)(1+N)\\ &\equiv (1-pA-N+pAN+N^2-N^3)(1+pA+N+pAN)\\ &\equiv 1+p[A,N]-pNAN\\ &\equiv 1+p[A,N]-pN[A,N]\\ &= 1+p\begin{bmatrix} -c & a-d-c\\ 0 & c\end{bmatrix}\end{aligned}$$

□

Lemma 4.2. *We have* $h_d^p \equiv 1 + p\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$ *mod* p^2.

Proof. We have $h_d = 1 + N$ with $N = \begin{bmatrix} p\,a_d & 1+p\,e\\ p\,c_d & p\,f\end{bmatrix}$ so that mod p^2

$$pN \equiv p\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}, \quad N^2 \equiv p\begin{bmatrix}0 & a_d+f\\ 0 & 0\end{bmatrix}, \quad N^3 \equiv 0.$$

Hence we have $h_d^p = (1+N)^p \equiv 1 + pN \mod p^2$. □

Let $M = \mathbb{Z}_p e_1 + \mathbb{Z}_p e_2$ and let B be the image of $A = \mathbb{Z}_p[[G_S]]$ in $\mathrm{End}(M)$. Let $J = (p, h_1 - 1, \ldots, h_d - 1)$ be the augmentation ideal of B. Then $JM = \mathbb{Z}_p e_1 + \mathbb{Z}_p p\, e_2$ and by induction we have

$$J^k M = \mathbb{Z}_p\, p^{k-1} e_1 + \mathbb{Z}_p\, p^k e_2$$

for $k \geq 1$. It follows that $\mathrm{gr}(M) = \sum_{k\geq 0} J^k M/J^{k+1}M$ is a free $\mathbb{F}_p[\pi]$-module with basis $\overline{e}_1 \in \mathrm{gr}_1(M), \overline{e}_2 \in \mathrm{gr}_0(M)$. Using the fact that

$$(h_i - 1)e_1 = p\,a_i e_1 + p\,c_i e_2$$

with $p^2 | c_i$ we see that $\mathrm{gr}(h_i - 1)\overline{e}_1 = a_i \pi \overline{e}_1$. Since the elements $\mathrm{gr}(h_i - 1)$, $(i \leq d)$ generate $\mathrm{gr}(B) = \sum_{k\geq 0} J^k/J^{k+1}$ the submodule $W = \mathbb{F}_p[\pi]\overline{e}_1$ is invariant under $\mathrm{gr}(B)$ and we obtain a homomorphism

$$\phi_1 : \mathrm{gr}(B) \to \mathrm{End}(W) = gl_1(\mathbb{F}_p[\pi])$$

with $\phi_1(\mathrm{gr}(h_i - 1)) = \pi a_i$. We want to show that a_i is non-trivial mod p for some $i < d$.

Lemma 4.3. *If* $X = 1 + pA \in \mathrm{SL}_n^{(1)}(\mathbb{Z}_p)$ *then* $\mathrm{tr}(A) \equiv 0$ *mod* p.

Proof. If $X = 1 + pN \in \mathrm{SL}_n^{(1)}(\mathbb{Z}_p)$, we have $1 = \det(1 + pN) \equiv 1 + p\,\mathrm{tr}(N)$ mod p^2 which implies that $\mathrm{tr}(N) \equiv 0$ mod p. □

Lemma 4.4. *If* $1 \leq i < d$ *and* $\pi a_i = \phi_1(\mathrm{gr}(h_i - 1)) = 0$ *then* $[h_i, h_d] \in \mathrm{SL}_2^{(2)}(\mathbb{Z}_p)$.

Proof. Since $a_i \equiv 0$ mod p, Lemma 4.3 implies that $d_i \equiv 0$ mod p. The result then follows from Lemma 4.1. □

Lemma 4.5. *If* $\pi a_i = \phi_1(\mathrm{gr}(h_i - 1)) = 0$ *for* $1 \leq i < d$ *then* $[H, H] \subseteq \mathrm{SL}_2^{(2)}(\mathbb{Z}_p)$.

Proof. The pro-p-group $[H,H]$ is generated, as a normal subgroup of H, by the elements of the form $[h_i,h_j]$ and $[h_i,h_d]$ with $i,j<d$. Since the elements of the form $[h_i,h_j]$ with $i,j<d$ are congruent to 1 mod p^2 by the proof of Lemma 3.2, the result follows from Lemma 4.4. □

So if $\mathrm{gr}(h_i-1)$ acts trivially on W for $1\le i<d$ then h_d^p is not in $[H,H]$ by Lemmas 4.5 and 4.2, contradicting the fact that $H/[H,H]$ is elementary. So the homomorphism $\phi_1:\mathrm{gr}(B)\to gl_1(\mathbb{F}_p[\pi])$ is non-trivial. Composing ϕ_1 with the canonical surjection $\mathrm{gr}(\mathbb{Z}_p[[G_S]])\to\mathrm{gr}(B)$, we obtain a non-trivial homomorphism

$$\phi:\mathrm{gr}(\mathbb{Z}_p[[G_S]])\to gl_1(\mathbb{F}_p[\pi]).$$

Composing the canonical map $\alpha:\mathrm{gr}(G_S)\to\mathrm{gr}(\mathbb{Z}_p[[G_S]])$ with ϕ, we get a Lie algebra homomorphism

$$\mathrm{gr}'(\rho):\mathrm{gr}(G_S)\to gl_1(\mathbb{F}_p[\pi]).$$

Since G_S is mild α is injective and $\mathrm{gr}(\mathbb{Z}_p[[G_S]])$ is the enveloping algebra of $\mathrm{gr}(G_S)$ which implies that $\mathrm{gr}'(\rho)\ne 0$ since $\mathrm{gr}(G_S)$ generates $\mathrm{gr}(\mathbb{Z}_p[[G_S]])$.

Now G_S has the presentation $F(x_1,\ldots,x_d)/(r_1,\ldots,r_d)$ where

$$r_i=x_i^{pc_i}\prod_{j\ne i}[x_i,x_j]^{\ell_{ij}} \mod F_3.$$

Since G_S is mild, we have $\mathrm{gr}(G_S)=<\xi_1,\ldots,\xi_n\mid\rho_1,\ldots\rho_d>$ where

$$\rho_i=c_i\pi\xi_i+\sum_{j\ne i}\ell_{ij}[\xi_i,\xi_j].$$

In this case, if $\mathrm{gr}'(\rho)(\xi_i)=\pi u_i$ then $\mathrm{gr}'(\rho)(\rho_i)=\pi^2c_iu_i=0$ and so $u_i=0$ for all i which contradicts the fact that $\mathrm{gr}'(\rho)\ne 0$.

5. Proof of Theorem 1.6

Here $|S|=3$ and the relations for $\mathfrak{l}_S$ can be written in the form

$$\begin{aligned}\xi_1&=m_{12}[\xi_1,\xi_2]+m_{13}[\xi_1,\xi_3],\\ \xi_2&=m_{21}[\xi_2,\xi_1]+m_{23}[\xi_2,\xi_3],\\ \xi_3&=m_{31}[\xi_3,\xi_1]+m_{32}[\xi_3,\xi_2],\end{aligned}$$

where $m_{ij}=-\ell_{ij}/c_i$. Let $r:\mathfrak{l}_S\to gl_n(\mathbb{F}_p)$ be a Lie algebra homomorphism and let $A_i=r(\xi_i)$. Then

$$\begin{aligned}A_1&=m_{12}[A_1,A_2]+m_{13}[A_1,A_3],\\ A_2&=m_{21}[A_2,A_1]+m_{23}[A_2,A_3],\\ A_3&=m_{31}[A_3,A_1]+m_{32}[A_3,A_2],\end{aligned}$$

Since $r=0$ if A_1,A_2,A_3 are linearly dependent we may assume that A_1,A_2,A_3 are linearly independent. Note that each of the above relations can be written in the form $A_i=[A_i,B_i]$ for some $B_i\in gl_n(\mathbb{F}_p)$. Then, by the following Lemma which was pointed out to us by Nigel Boston, each matrix A_i is nilpotent if $n<p$.

Lemma 5.1. *Let A,B be $n\times n$ matrices over $\mathbb{F}_p$ with $A=[A,B]$. Then A is nilpotent if $n<p$.*

Proof. Replacing $\mathbb{F}_p$ be a finite extension $\mathbb{F}_q$, we may assume that A is upper triangular. Then the trace of A^{q-1} is $k \cdot 1$ with $0 \le k < p$. But the trace of A^n is zero for any $n \ge 1$ since $A = [A, B]$ implies that $\mathrm{tr}(A^n) = \mathrm{tr}(ABA^{n-1} - BA^n) = 0$. It follows that $k = 0$ and hence that the characteristic polynomial of A is X^n. □

Remark. This proof of the above Lemma is due to Julien Blondeau.

If condition (a) holds we can, without loss of generality, assume that $m_{12} = 0$. Then $A_1 = [A_1, B_1]$ with $B_1 = m_{13}A_3$ nilpotent which implies $\mathrm{ad}(B_1)$ nilpotent. Hence $A_1 = 0$ and we are reduced to the case $|S| = 2$.

If condition (b) holds we can, without loss of generality, assume that $m_{13} = m_{23}$. Taking a linear combination of the first two equations we obtain

$$aA_1 + bA_2 = (am_{12} - bm_{21})[A_1, A_2] + [aA_1 + b\frac{m_{23}}{m_{13}}A_2, m_{13}A_3].$$

Choose non-zero $a, b \in \mathbb{F}_p$ so that $am_{12} - bm_{21} = 0$. Then

$$aA_1 + bA_2 = [aA_1 + bA_2, m_{13}A_3]$$

which implies $aA_1 + bA_2 = 0$ since $\mathrm{ad}(A_3)$ is nilpotent. We can then write the equations in the form $A_2 = c[A_2, A_3]$, $A_2 = d[A_2, A_3]$, $A_3 = e[A_2, A_3]$ from which we readily get $A_1 = A_2 = A_3 = 0$.

If condition (c) holds we may, without loss of generality, assume that $m_{23} \ne m_{13}$ and $m_{32}m_{21} \ne m_{31}m_{12}$. For non-zero $a, b \in \mathbb{F}_p$ we consider the equation

$$aA_1 + bA_2 + A_3 = (am_{12} - bm_{21})[A_1, A_2] + (am_{13} - m_{31})[A_1, A_3] + (bm_{23} - m_{32})[A_2, A_3].$$

Let $b = m_{12}a/m_{21}$ and choose λ such that $am_{13} - m_{31} = \lambda a$. Then

$$\begin{aligned} bm_{23} - m_{32} = \lambda b &\iff am_{12}m_{23}/m_{21} - m_{32} = \lambda am_{12}/m_{21} \\ &\iff am_{12}m_{23} - m_{32}m_{21} = m_{12}(am_{13} - m_{31}) \\ &\iff am_{12}(m_{23} - m_{13}) = m_{32}m_{21} - m_{12}m_{31} \\ &\iff a = \frac{m_{32}m_{21} - m_{31}m_{12}}{m_{12}(m_{23} - m_{13})}. \end{aligned}$$

With this choice of a we have

$$aA_1 + bA_2 + A_3 = [\lambda aA_1 + \lambda bA_2, A_3] = [aA_1 + bA_2 + A_3, \lambda A_3]$$

which implies $aA_1 + bA_2 + A_3 = 0$ since $\mathrm{ad}(A_3)$ is nilpotent.

If conditions (a), (b), (c) fail then

$$\begin{vmatrix} m_{31} & m_{32} \\ m_{21} & m_{12} \end{vmatrix} = \begin{vmatrix} m_{12} & m_{13} \\ m_{32} & m_{23} \end{vmatrix} = \begin{vmatrix} m_{21} & m_{23} \\ m_{31} & m_{13} \end{vmatrix} = 0$$

which implies

$$m_{31} = k_1 m_{21},\ m_{32} = k_1 m_{12},\ m_{12} = k_2 m_{32},\ m_{13} = k_2 m_{23},\ m_{21} = k_3 m_{31},\ m_{23} = k_3 m_{13}$$

for some $k_1, k_2, k_3 \in \mathbb{F}_p^*$. This implies that $k_i k_j = 1$ for all $i \ne j$ and hence that $k_i^2 = 1$ for all i. Since, by hypothesis, $k_i \ne 1$ we must have $k_i = -1$ for all i. Then the relators for $\mathfrak{l}_S$ are of the form

$$\xi_1 = a[\xi_1, \xi_2] + b[\xi_1, \xi_3],$$
$$\xi_2 = c[\xi_2, \xi_1] - b[\xi_2, \xi_3],$$
$$\xi_3 = -c[\xi_3, \xi_1] - a[\xi_3, \xi_2]$$

with $a, b, c \in \mathbb{F}_p^*$. After the transformation $\xi_1 \mapsto c^{-1}\xi_1$, $\xi_2 \mapsto a^{-1}\xi_2$, $\xi_3 \mapsto b^{-1}\xi_3$ the relations become

$$\xi_1 = [\xi_1, \xi_2] + [\xi_1, \xi_3],$$
$$\xi_2 = [\xi_2, \xi_1] - [\xi_2, \xi_3],$$
$$\xi_3 = -[\xi_3, \xi_1] - [\xi_3, \xi_2]$$

But these relations are satisfied if we replace ξ_i by $A_i \in gl_2(\mathbb{F}_p)$ with

$$A_1 = -\frac{1}{2}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad A_2 = -\frac{1}{2}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad A_3 = -\frac{1}{2}\begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix}$$

which yields an isomorphism of $\mathfrak{l}_S$ with $sl_2(\mathbb{F}_p)$.

Thus the only case where Property $FM(n)$ would fail would be when $\ell_{ij} \neq 0$ for all i, j and

$$\ell_{13}/c_1 = -\ell_{23}/c_2, \ \ell_{21}/c_2 = -\ell_{31}/c_3, \ \ell_{12}/c_1 = -\ell_{32}/c_3.$$

Note that, since $q_i \equiv g_j^{-\ell_{ij}} \mod q_j$, this is equivalent to

$$(q_1^{c_2} q_2^{c_1})^{c_3} \equiv 1 \mod q_3, \quad (q_2^{c_3} q_3^{c_2})^{c_1} \equiv 1 \mod q_1, \quad (q_1^{c_3} q_3^{c_1})^{c_2} \equiv 1 \mod q_2.$$

6. Proof of Theorem 2.6

By Theorem 2.4, we can find a set of primes $S' = \{q'_1, \ldots, q'_{2d}\}$ such that $q'_{2i} = q_i$ and $\ell'_{i,i+1} \neq 0$ if i odd, $\ell'_{i,i+1} \neq 0$ if $i < 2d$ is even and $\ell'_{2d,1} \neq 0$ with all other $\ell'_{i,j} = 0$ if i or j is odd. If f is a homomorphism of $\mathfrak{l}_{S'}$ into $gl_n(\mathbb{F}_p)$ let $A_i = f(\xi_i)$. Then $a_i A_i + [A_i, A_{i+1}] = 0$ for some non-zero a_i if i is odd and $A_i = [A_i, B_i]$ for some matrix B_i if i is even. By Lemma 5.1 this implies that A_i is nilpotent if i is even and hence that $\mathrm{ad}(A_i)$ is nilpotent if i is even. But this implies that $A_i = 0$ if i is odd. That $G_{S'}$ is mild follows from the fact that S' is a circular set of primes.

7. Proof of Theorem 1.9

Let ρ be a continuous homomorphism of G into $\mathrm{GL}_n^{(1)}(\mathbb{Z}_p)$. If $\rho(x_i) = 1 + pA_i$ then, modulo p^3, we have $\rho(r_i) = 1 + p^2(c_1 A_i + [A_i, A_{i+1}]) = 0$ if $i < 2m$ and

$$\rho(r_{2m}) = 1 + p^2(c_{2m} A_{2m} + [A_{2m}, A_1]) = 0.$$

Hence, if $\overline{A}_i$ is the image of A_i in $gl_n(\mathbb{F}_p)$, we have

$$c_1\overline{A}_1 + [\overline{A}_1, \overline{A}_2] = 0, \ c_2\overline{A}_2 + [\overline{A}_2, \overline{A}_3] = 0, \cdots, c_{2m}\overline{A}_{2m} + [\overline{A}_{2m}, \overline{A}_1] = 0$$

By Lemma 5.1 we see that $\mathrm{ad}(\overline{A}_i)$ is nilpotent for all i and hence $\overline{A}_i = 0$ for all i. But this implies $\rho = 1$ since $\rho \neq 1$ implies $\overline{A}_i \neq 0$ for some i by Lemma 3.2.

References

[1] J-M. Fontaine and B. Mazur, *Geometric Galois representations, elliptic curves, modular forms and Fermat's last theorem.* (Hong Kong 1993), 41-48, Ser. Number Theory, I, Internat, Press, Cambridge, MA, 1995.

[2] H. Koch, *Galois Theory of p-Extensions*, Springer Verlag, 2002.

[3] J. Labute, *Mild pro-p-groups and Galois groups of p-extensions of* $\mathbb{Q}$, J. Reine Angew. Math. 596 (2006), 115-130.

Department of Mathematics and Statistics, McGill University, Burnside Hall, 805 Sherbrooke Street West, Montreal QC H3A 0B9, Canada

E-mail address: labute@math.mcgill.ca