A FAMILY OF p-ADIC ANALYTIC TAME p-CLASS TOWERS

JOHN LABUTE

ABSTRACT. Let p be an odd prime, let S be a finite 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 $|S| = 3$ and $[G_S, G_S] \subseteq G_S^p$ we show that the linking algebra $\mathfrak{l}_S$ is either $sl_2(\mathbb{F}_p)$, in which case G_S is p-adic analytic, or 0 in which case $|G_S| \leq p^9$.

Let p be an odd prime, let $S = \{q_1, q_2, q_3\}$ be a finite 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. The pro-p-group G_S has a presentation $F(x_1, x_2, x_3)/(r_1, r_2, r_3)$ where x_i is a lifting of a generator of an inertia group at q_i and

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

with $c_i = (q_i - 1)/p \not\equiv 0 \bmod p$ and the linking number ℓ_{ij} of (q_i, q_j) defined by $q_i \equiv g_j^{-\ell_{ij}} \bmod q_j$ with g_j a primitive root mod q_j and where F_3 the third term of the descending p-central series of the free pro-p-group $F = F(x_1, x_2, x_3)$, cf. Koch [3], Example 11.11.

Let $\mathfrak{g}_S$ be the finitely presented Lie algebra over $\mathbb{F}_p[\pi]$ generated by ξ_1, ξ_2, ξ_3 with relators ρ_1, ρ_2, ρ_3 where

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

The Lie algebra $\mathfrak{g}_S$ has as a quotient $\mathrm{gr}(G_S)$, the Lie algebra associated to the descending p-central series of G_S. A related Lie algebra is the finitely presented Lie algebra $\mathfrak{l}_S$ over $\mathbb{F}_p$ generated by ξ_1, ξ_2, ξ_3 with relators $\sigma_1, \sigma_2, \sigma_3$ where

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

We call this Lie algebra the **linking algebra** of S.

The set S is said to be **powerful** if $\ell_{12}\ell_{23}\ell_{31} \neq \ell_{13}\ell_{32}\ell_{21}$. This s equivalent to

$$[\mathfrak{g}_S, \mathfrak{g}_S] \subseteq \pi \mathfrak{g}_S$$

which in turn is equivalent to $[G_S, G_S] \subseteq G_S^p$, i.e. that G_S is a powerful pro-p-group.

The set S is said to be **uniform** if $\ell_{ij} \neq 0$ for all i, j and

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

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

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

Date: June 27, 2022.

2020 *Mathematics Subject Classification.* 11R34, 20E15, 12G10, 20F05, 20F14, 20F40.

For example, using PARI/GP, we found that S is uniform 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: if $p = 7$ and the primes in S are at most 104707, the set S is uniform about .2% of the time and powerful approximately 80% of the time.

Theorem 1. *If S is powerful then either $\mathfrak{l}_S = 0$ or $\mathfrak{l}_S \cong sl_2(\mathbb{F}_p)$. We have $\mathfrak{l}_S = 0$ if and only if S is not uniform.*

Lemma 2. *If $\mathfrak{l}$ is a three dimensional Lie algebra over $\mathbb{F}_p$ ($p \neq 2$) with $\mathfrak{l} = [\mathfrak{l}, \mathfrak{l}]$ then $\mathfrak{l} \cong sl_2(\mathbb{F}_p)$.*

Proof. By [5], page 13, and the classification of quadratic forms over $\mathbb{F}_p$ for $p \neq 2$ there is a basis e_1, e_2, e_3 for $\mathfrak{l}$ such that

$$[e_2, e_3] = e_1, [e_3, e_1] = e_2, [e_1, e_2] = \delta e_3$$

with $\delta \neq 0$. If $h = a_1e_1 + a_2e_2 + a_3e_3$ the characteristic polynomial of $\mathrm{ad}(h)$ is

$$\lambda(\lambda^2 + a_1^2 + \delta^2 a_2^2 + a_3^2).$$

Since the equation $a_1^2 + \delta^2 a_2^2 + a_3^2 = -1$ always has a solution we obtain a non-zero $f \in \mathfrak{l}$ with $[h, f] = f$ which is enough to show that $\mathfrak{l} \cong sl_2(\mathbb{F}_p)$; cf. [5], page 14. □

Proof of Theorem 1. If S is powerful then either $\mathfrak{l}_S = 0$ or $\mathfrak{l}_S$ has dimension 3 in which it is isomorphic to $sl_2(\mathbb{F}_p)$ by Lemma 2. If S is not uniform then by [6], Theorem 1.7, every 2-dimensional representation of $\mathfrak{l}_S$ is trivial which shows that $\mathfrak{l}_S = 0$. □

Theorem 3. *If S is powerful but not uniform then $|G_S| \leq p^9$.*

Proof. If S is powerful but not uniform then, using the fact that

$$\mathfrak{g}_S \otimes_{\mathbb{F}_p[\pi]} \mathbb{F}_p(\pi) \cong \mathfrak{l}_S \otimes_{\mathbb{F}_p} \mathbb{F}_p(\pi),$$

we obtain the fact that $\mathfrak{g}_S$ is a finitely generated torsion $\mathbb{F}_p[\pi]$-module which implies that $\mathfrak{g}_S$ is finite. Hence $\mathrm{gr}(G_S)$, which is a quotient of $\mathfrak{g}_S$, is finite which implies the finiteness of G_S.

Suppose that $|G_S| > p^9$. Then $\pi^2 : \mathrm{gr}_1(G_S) \to \mathrm{gr}_3(G_S)$ is an isomorphism. Otherwise, there exists a basis η_1, η_2, η_3 of $\mathrm{gr}_1(G_S)$ with $\pi^2\eta_1 = 0$ so that the dimension of $\mathrm{gr}_3(G_S)$ is less that 3. Then since

$$\pi : \mathrm{gr}_1(G_S) \to \mathrm{gr}_2(G_S)$$

is an isomorphism, the elements $\zeta_1 = \pi^{-1}[\eta_1, \eta_2]$, $\zeta_2 = \pi^{-1}[\eta_1, \eta_3]$ are linearly independent over $\mathbb{F}_p$. But then $\pi^3\zeta_1 = \pi^3\zeta_2 = 0$ which shows that the dimension of $\mathrm{gr}_4(G_S)$ is less than 2. Completing ζ_1, ζ_2 to a basis $\zeta_1, \zeta_2, \zeta_4$ of $\mathrm{gr}_1(G)$, the elements τ_1, τ_2, τ_3 defined by

$$\tau_1 = \pi^{-1}[\zeta_2, \eta_3],\ \tau_2 = \pi^{-1}[\zeta_1, \zeta_3],\ \tau_3 = \pi^{-1}[\zeta_1, \zeta_2]$$

form a basis of $\mathrm{gr}_1(G_S)$ and $\pi^4\tau_i = 0$ for all i which shows that $\mathrm{gr}_5(G_S) = 0$. Hence the dimension of $\mathrm{gr}(G_S)$ is at most 9 which implies that $|G_S| \leq p^9$, a contradiction.

Since $\pi^2 : \mathrm{gr}_1(G_S) \to \mathrm{gr}_3(G_S)$ is an isomorphism, $\mathrm{gr}_1(G_S)$ is a Lie algebra over $\mathbb{F}_p$ under the bracket $< \xi, \eta >= \pi^{-1}[\xi, \eta]$. But the relations for $\mathfrak{g}_S$ then imply that, with this Lie algebra structure, $\mathrm{gr}_1(G_S)$ is a quotient of $\mathfrak{l}_S$ which is zero since S is not uniform. But this contradicts the fact that $\mathrm{gr}_1(G_S) \neq 0$ □

In [1] Andozskii and Cvetkov show that if G is a powerful pro-p-group with 3 generators and 3 relations and with $G/[G,G] \cong (\mathbb{Z}/p\mathbb{Z})^3$ then either G is finite or G is isomorphic to

$$\mathrm{SL}_2^{(1)}(\mathbb{Z}_p) = \{A \in \mathrm{SL}_2(\mathbb{Z}_p) \mid A \equiv 1 \bmod p\}.$$

The following gives another proof of the fact that G_S is p-adic analytic if G_S is infinite in the case that S is uniform.

Theorem 4. *If S is uniform then $\mathfrak{g}_S$ is a free $\mathbb{F}_p[\pi]$ module on ξ_1, ξ_2, ξ_3.*

Proof. Since $[\xi_i, \xi_j]$ is a linear combination of $\pi\xi_1, \pi\xi_2, \pi\xi_3$ in $\mathfrak{g}_S$ it follows that, as an $\mathbb{F}_p[\pi]$-module, $\mathfrak{g}_S$ is generated by ξ_1, ξ_2, ξ_3. They form a basis for $\mathfrak{g}_S$ since their images in

$$\mathfrak{g}_S \otimes_{\mathbb{F}_p[\pi]} F_p(\pi) \cong sl_2(\mathbb{F}_p(\pi))$$

are linearly independent. ☐

Theorem 5. *If S is uniform and G_S is infinite the map $\phi : \mathfrak{g}_S \longrightarrow \mathrm{gr}(G_S)$ is an isomorphism.*

Proof. If S is uniform and G_S infinite the surjective map

$$\mathfrak{g}_S \otimes_{\mathbb{F}_p[\pi]} F_p(\pi) \longrightarrow \mathrm{gr}(G_S) \otimes_{\mathbb{F}_p[\pi]} F_p(\pi)$$

is an isomorphism since $\mathfrak{g}_S \otimes_{\mathbb{F}_p[\pi]} \mathbb{F}_p(\pi) \cong sl_2(F_p(\pi))$, a simple Lie algebra, and $\mathrm{gr}(G_S) \otimes_{\mathbb{F}_p[\pi]} F_p(\pi) \neq 0$. But this implies that ϕ is an isomorphism. ☐

Thus, if S is uniform and G_S infinite, the Lie algebra $\mathrm{gr}(G_S)$ is a free $\mathbb{F}_p[\pi]$-module on ξ_1, ξ_2, ξ_3. But this implies that G_S is a uniform pro-p-group and hence an analytic pro-p-group. See [4] for the theory of uniform pro-p-groups.

It is not known if G_S can be infinite when S is uniform. The Fontaine-Mazur Conjecture (cf. [2]) implies that it it is finite. For example, if $p = 3$ and S=$\{$7,31,229$\}$ then G_S is p-adic analytic but it is not known whether G_S is finite or not.

References

[1] I. Andozskii and V. Cvetkov, *On a series of finite p-closed p-groups*, Math. USSR Izv. 8 (1974), 285-297.

[2] 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.

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

[4] J.D. Dixon, M.P.F. du Sautoy, A. Mann, D. Segal, *Analytic Pro-p-Groups (2nd edition)*, Cambridge Studies in Advanced Mathematics 61, Cambridge University Press, 2003.

[5] N. Jacobson, Lie algebras. Interscience Tracts in Pure and Applied Masthematics 10, Interscience Publishers, 1962.

[6] J. Labute, Linking Numbers and the Tame Fontaine-Mazur Conjecture, Annales Math. du Quebec, (to appear).

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

Email address: labute@math.mcgill.ca