On just infinite pro-p-groups and arithmetically profinite extensions of local fields

Ivan Fesenko

0. Introduction.

Let F be a local field of characteristic $p > 0$ with perfect residue field k. The wild group $R = \mathrm{Aut}_1 F$ is the group of wild continuous automorphisms $\{\sigma : (\sigma - 1)\mathcal{O}_F \subset \mathcal{M}_F^2\}$ of the local field F. A choice of a prime element t of a local field F determines an isomorphism of $\mathrm{Aut}_1 F$ and the group of formal power series $f(t) = t + a_2 t^2 + \dots$ with coefficients from k with respect to the composition $(f \circ g)(t) = f(g(t))$. We shall write R_k for R to specify the residue field.

The group R_k plays an important role in the theory of pro-p-groups. Recall that an infinite pro-p-group is called just infinite if it has no proper infinite quotients. It is easy to show that every finitely generated pro-p-group has a just infinite quotient. Just infinite groups of finite width (the lower central series have bounded orders) are split into three families (see for instance [18]): (i) those which are analytic over $\mathbb{Z}_p$; (ii) those which are analytic over other infinite commutative noetherian local rings which are integral domains with finite residue field; (iii) the rest. The wild group R_k belongs to the latter family (for a complete proof see section 5 of [32]). If Fontaine–Mazur–Boston's conjecture holds (see [2]), every just infinite pro-p-quotient of the Galois group of the maximal unramified outside a finite set of primes of a finite extension of $\mathbb{Q}$ none of which lies over p should belong to the third family.

Group theoretists sometimes call R_k the Nottingham group. It has been investigated by group theoretical methods (D. Johnson, I. York, A. Weiss, C. Leedham-Green, A. Weiss, A. Shalev, R. Camina, Y. Barnea, B. Klopsch) and number theoretical methods (Sh. Sen, J.-M. Fontaine, J.-P. Wintenberger, F. Laubie).

This paper consists of two parts.

In the first part, sections 1 – 5, we apply Fontaine–Wintenberger's theory of fields of norms to study the structure of the wild group R_k. In particular we provide a new short proof of R. Camina's theorem which says that every countably based pro-p-group (i.e. with countably many open subgroups) is isomorphic to a closed subgroup of $R_{\mathbb{F}_p}$.

Crelle's Journal 517(1999), 61–80 © IF

The proof is an immediate corollary of Proposition of section 5: every pro-p-group with countably many open subgroups is realizable as the Galois group of an arithmetically profinite extension of a local field of characteristic p. Lubotzky–Wilson's theorem is deduced as another corollary. It is interesting to investigate which finitely generated pro-p-groups are realizable as the Galois group of an arithmetically profinite extension of a local field of characteristic 0. Due to Sen [25] p-adic Lie groups are; another realizable set of groups $T[r]$ is provided in this work.

In the second part, sections 6 – 8, we study specific subgroups $T[r]$ of $R_{\mathbb{F}_p}$. Fix a power p^r and define $T = T[r] = \left\{\sum_{i\geqslant 0} a_i t^{1+p^r i} : a_0 = 1, a_i \in \mathbb{F}_p\right\}$. These subgroups of $R_{\mathbb{F}_p}$ have various bizarre properties, sometimes similar to those of p-adic Lie groups. At the same time, the commutator subgroup is unusually small and the abelian quotient is of exponent greater than p which is important for number theory applications. Section 6, the longest in this work, is filled with combinatorial arguments required for the study of $T[r]$. Subgroups $T[r]$ are torsion free and don't belong to the first family of just infinite pro-p-groups; most likely they are in the third family.

In section 7 we realize the group $T[r]$ for $r \geqslant 2$ as the Galois group of an arithmetically profinite extensions of $\mathfrak{p}$-adic fields. We answer affirmatively in section 8 Coates–Greenberg's problem on deeply ramified extensions of local fields stated in [5].

I am thankful to Moshe Jarden and Shankar Sen for their suggestions which helped greatly improve the exposition and to Marcus du Sautoy for several discussions. For a leisurely introduction to various topics related to this work see [33].

This study of deeply ramified extensions and Coates–Greenberg's problem was initiated by a dinner question of Jürgen Neukirch in June 1994 during a number theory conference in Oberwolfach and following conversations with John Coates and Ralph Greenberg. I am very grateful to them for numerous discussions and continuous encouragements.

1. The wild group.

Let v_F be the discrete valuations of $F = k((t))$. We use simultaneously two interpretations of $R = R_k$: as formal power series $t + a_2 t^2 + \dots$ with respect to the composition and as wild automorphisms of F. When we use formal power series f, g their multiplication is denoted by $f \circ g$, when we use automorphisms σ, τ their product in R is denoted by $\sigma\tau$.

For a formal power series $f(t)$ denote $i(f(t)) = \min\{i \geqslant 2 : a_i \neq 0\} - 1$. Let $R_i = \{f(t) : i(f(t)) \geqslant i\}$.

Denote $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$. The following property of commutators is useful

$$[\sigma\tau, \rho] = [\sigma, [\tau, \rho]][\tau, \rho][\sigma, \rho].$$

As usual, we denote by dots terms of higher order. For $a, b \in k$

$$[t + at^i, t + bt^j] = t + ab(i - j)t^{i+j-1} + \dots.$$

Therefore, R_i are normal subgroups of R. The group R being the projective limit of finite p-groups R/R_i is a pro-p-group. From the commutator formula one immediately deduces

that $[R_n, R_m] = R_{n+m}$ if $m-n$ is relatively prime to p and $[R_n, R_m] = R_{n+m+1}$ if $m-n$ is divisible by p, see for example [7], Prop. 12. In addition, $R_n^p \leqslant R_{np}$, see the proof of part (1) of the theorem in section 6. Thus, $[R,R] = [R,R]R^p = R_3$. The group $R_{\mathbb{F}_p}$ is a pro-p-group with 2 generators, generated by any two elements of $R_1 \setminus R_2$ and $R_2 \setminus R_3$, hence by $t+t^2$ of infinite order and $t/(1-t)$ of order p (note that any of their quotients is in $R_2 \setminus R_3$).

Moreover, the group R is a so called hereditarily just infinite group: every non-trivial normal closed subgroup G of an open subgroup is open. Indeed, to use the commutator formula above put $\sigma = t + at^{i+1}$, $\sigma\tau = t + at^{i+1} + \dots$, $\rho = t + bt^{j+1}$. Then $[t + at^{i+1} + \dots, t + bt^{j+1}] = t + ab(i-j)t^{i+j+1} + \dots$. Hence the set $H = [t + at^{i+1} + \dots, R_j]$ has the property $R_u \leqslant R_{u+1}H$ for $u \geqslant j+i, (p, u-i) = 1$. Then for an odd p and sufficiently large l the group G contains some $t + at^l + \dots$ and $t + at^{l+1} + \dots$, so G contains R_w for sufficiently large w. For $p = 2$ use in the property $(t + at^i) \circ (t + at^i) = t + a^2t^{2i-1} + \dots$.

For additional remarks and illustrative examples see [33].

2. Theorem of Sen.

For a closed subgroup G of R put $G_i = G \cap R_i$ for $i \in \mathbb{N}$, $G_x = G_{\lceil x \rceil}$ for $x \in \mathbb{R}$. Denote $\varphi_G(x) = \int_0^x \frac{dy}{|G:G_y|}$. The group G is called an arithmetically profinite subgroup of R if $\lim_{x \to +\infty} \varphi_G(x) = +\infty$, see [27]. If this is the case, define $\psi_G(x)$ as the inverse function to $\varphi_G(x)$ and put $G(x) = G_{\psi_G(x)}$. The points of discontinuity of the derivative of φ_G are called breaks of G; the points of discontinuity of the derivative of ψ_G are called upper breaks of G.

A theorem of Sen [24] says that the subgroup of G generated by an element σ of infinite order is arithmetically profinite and $i(\sigma^{p^n}) \equiv i(\sigma^{p^{n-1}}) \mod p^n$. For generalizations and other proofs see [29], [20], [19]. For a leisurely discussion of Sen's theorem see [33].

3. Fields of norms of arithmetically profinite extensions.

Let K be a local field with perfect residue field $k = k_K$ of characteristic p. A Galois extension L/K is called arithmetically profinite if the upper ramification groups $G(L/K)^x$ are open in $G(L/K)$ for every x. Equivalently, L/K is arithmetically profinite if it has finite residue field extension and the Hasse–Herbrand function $h_{L/K}(x) = \lim h_{E/K}(x)$ takes real values for all real $x \geqslant 0$ where E/K runs through all finite subextensions in L/K, see [30]; [9], Ch. III, sect. 5.

For an infinite Galois arithmetically profinite extension L/K the field of norms $N = N(L/K)$ is the set of all norm-compatible sequences

$$\{(a_E) : a_E \in E^*, E/K \text{ is a finite subextension of } L/K\}$$

and zero, such that the multiplication is componentwise and the addition $(a_E) + (b_E) = (c_E)$ is defined as $c_E = \lim_M N_{M/E}(a_M + b_M)$ where M runs through all finite subextension of E in L. For the properties of the fields of norms see [27]; [30]; [9], Ch. III, sect. 5.

In this paper with sections 7 and 8 excluded all Galois arithmetically profinite extensions are totally ramified p-extensions; therefore the Galois group consists of wild automorphisms only.

The field N is a local field of characteristic p with the residue field k_L and a prime element $t = (\pi_E)$ which is a sequence of norm-compatible prime elements of finite subextensions of L/K. Every automorphism τ of L over K being wild induces a wild automorphism σ of the field of norms: $\sigma((\pi_E)) = (\tau\pi_E)$.

A Galois infinite subextension of a Galois arithmetically profinite extension is arithmetically profinite. Let F/K be a Galois totally ramified p-extension and F contain L which is an arithmetically profinite extension of K. If $|F : L| < +\infty$, then F/K is an arithmetically profinite extension. The field of norms $N(L/K)$ can be identified with a subfield of $N(F/K)$; the extension $N(F/K)/N(L/K)$ is an extension of local fields. If F is a Galois extension of L, then one defines $N(F, L/K)$ as the compositum of all $N(F'/K)$ where F' runs through Galois extensions of K in F with $|F' : L| < +\infty$. One of the central theorems of the theory of fields of norms says that the absolute Galois group of $N(L/K)$ coincides with $G(N(L^{\rm sep}, L/K)/N(L/K))$ and the latter is isomorphic to $G(L^{\rm sep}/L)$, see [30], (3.2.2).

The functor of field of norms $W = W_{L/K}$ associates to an infinite Galois arithmetically profinite extension L/K its field of norms $N(L/K)$ and the closed arithmetically profinite subgroup G of the group $R_k = \mathrm{Aut}_1 N(L/K)$ which is the image of the Galois group of L/K; the upper ramification filtration $G(L/K)^x$ is mapped onto the filtration $G(x)$ of G, see [30], (3.3).

For a finite Galois totally ramified p-extension N/K of local fields of characteristic p the Galois group $G(N/K)$ is isomorphic to a subgroup of $R_k = \mathrm{Aut}_1 N$. The extension F/K is arithmetically profinite if and only if $N(F, L/K)$ is an arithmetically profinite extension of $N(L/K)$; then the image of the group $G(N(F, L/K)/N(L/K))$ under $W_{N(F,L/K)/N(L/K)}$ in R_k coincides with the image of $G(F/L)$ as a closed subgroup in $G(F/K)$ in R_k under $W_{F/K}$, see [30], (3.2).

4. Theorem of Wintenberger.

A theorem of Wintenberger ([29]) says that for every abelian closed subgroup G of the group R_k there exists a Galois arithmetically profinite extension L/K of local fields such that $W(L/K) = (k((t)), G)$.

For example, the group topologically generated by an element σ of infinite order in R comes from an arithmetically profinite $\mathbb{Z}_p$-extension L/K. It is easy to deduce that the sequence $i(\sigma^{p^n})/p^n$ is increasing. Denote $pe/(p-1) = \lim i(\sigma^{p^n})/p^n$. Then either $e = +\infty$ or $e \in \mathbb{N}$. In the first case K is of positive characteristic, in the second case K is of characteristic 0 and its absolute ramification index is e. By the proposition in section 6 $e(\tau) = (p-1)i$ is finite for $\tau(t) = t + t^{1+pi}$.

An observation due to Fontaine [10] is that $e = +\infty$ if and only if σ belongs to the topological closure of the torsion (the set of torsion elements) of R. Indeed, assume that

the group G topologically generated by σ comes from a Galois arithmetically profinite extension L/K of fields of characteristic p with a generator τ. Let K_n be the subextension of L of degree p^n over K. Map K_n isomorphically onto N by sending a prime element π_{K_n} of a norm-compatible sequence of prime elements of finite subextensions in L/K to t. Let $N_n \subset N$ be the image of K under this homomorphism, and let σ_n (of order p^n) be the image of τ. Then $i(\sigma\sigma_n^{-1})$ tends to $+\infty$ when n grows. Conversely, if σ is the limit of a sequence of automorphisms σ_n of finite order, then the upper breaks u_i of $G = \overline{(\sigma)}$ satisfy $u_{i+1} \geqslant u_i^p$ (see for instance [16]), therefore $e = +\infty$.

Wintenberger and Laubie studied p-adic Lie subgroups in R which are in the image of the functor W, see [27], [28], [15].

5. *Theorem of Camina and Theorem of Lubotzky and Wilson.*

The wild group R is not p-adic Lie, since for instance for every n relatively prime to p there is $\sigma \in R_n \setminus R_{n+1}$ such that $\sigma^p = e$ (it suffices to observe that given a natural number relatively prime to p there a cyclic totally ramified extension of degree p of a local field of characteristic p with the ramification break equal to that number). Another way to argue is to use the property of p-adic Lie groups to contain an open subgroup of finite rank (i.e. an open subgroup for which the supremum of the number of generators of its closed subgroups is not infinity), see [6], Cor. 9.36. The group R doesn't contain an open subgroup of finite rank, since the number of generators of R_i tends to infinity when i tends to infinity.

For more properties of R see Remark in section 6.

Proposition. Let G be a countably based pro-p-group. Then there exists a Galois arithmetically profinite extension L of $\mathbb{F}_p((X))$ such that $G(L/\mathbb{F}_p((X)))$ is isomorphic to G.

Proof. Let $G = \varprojlim G_i$ where G_i are finite pro-p-groups such that the kernel of the epimorphism $G_{i+1} \to G_i$ is of order p. Assume that G_i is isomorphic to $G(K_i/\mathbb{F}_p((X)))$. It is well known that the pro-p-part of the absolute Galois group of $\mathbb{F}_p((X))$ is a free countably generated pro-p-group. Non-positive powers of X of degree relatively prime to p form a basis of the vector space $\mathbb{F}_p((X))/\wp(\mathbb{F}_p((X)))$, where $\wp(x) = x^p - x$, over $\mathbb{F}_p$ (see, for instance, arguments in [9], Ch. IV, (5.4)), so it is of infinite dimension. Hence the imbedding problem $(G_{i+1} \to G_i = G(K_i/\mathbb{F}_p((X))))$ has a solution $K_i(\beta)$ with $\wp(\beta) = \alpha \in K_i$, see for instance [12], Th.1'. Following the method of Camina [3] replace α by $\alpha_1 = \alpha + c$ with $c \in \mathbb{F}_p((X))$. Then $K_{i+1} = K_i(\beta_1)$ with $\wp(\beta_1) = \alpha_1$ is a solution of the same imbedding problem. Let π_i be a prime element of K_i and O_i be its ring of integers. Due to the Artin–Schreier theory the kernel of $\mathbb{F}_p((X))/\wp(\mathbb{F}_p((X))) \to K_i/\wp(K_i)$ is finite dimensional, so for every k the kernel of $\mathbb{F}_p((X))/\wp(\mathbb{F}_p((X))) \to K_i/(\wp(K_i)+\pi_i^k O_i)$ is finite dimensional. Then the ramification break of K_{i+1}/K_i can be made arbitrarily large by choosing c not in $\wp(K_i) + \pi_i^{-k} O_i$ for sufficiently large k. Therefore one can construct an arithmetically profinite extension $L/\mathbb{F}_p((X))$ as desired. $\square$

Corollary 1 (Camina). Every countably based pro-p-group is isomorphic to a closed subgroup of $R_{\mathbb{F}_p}$.

Proof. Apply the functor W to the extension $L/\mathbb{F}_p((X))$. $\square$

Remark 1. According to the proof given in this paper every countably based pro-p-group is isomorphic to infinitely many different closed arithmetically profinite subgroups in the closure of the torsion of $R_{\mathbb{F}_p}$. Note that if $\tau \in G(L/\mathbb{F}_p((X)))$ is of infinite order, then the fixed field L_τ of τ is an arithmetically profinite extension of $\mathbb{F}_p((X))$. If it is infinite, the image of τ in $R_{\mathbb{F}_p}$ can be identified with the image of $\tau \in G(N(L, L_\tau/\mathbb{F}_p((X)))/N(L_\tau/\mathbb{F}_p((X))))$ in $R_{\mathbb{F}_p}$. The latter belongs to the closure of the torsion of $R_{\mathbb{F}_p}$ as was indicated in the previous section. Varying the set of upper ramification breaks as in the proposition every infinite countably based pro-p-group can be embedded in infinitely many ways into R; the images have different sets of breaks.

Remark 2. In Camina's proof every finitely generated pro-p-group is realized as the Galois group of a totally ramified p-extension with specific properties of its ramification breaks, then it is embedded into $R_{\mathbb{F}_p}$ (actually in the closure of the torsion). Then Lubotzky–Wilson's theorem is applied (see Corollary 2) to handle the general case of a countably based pro-p-group. One can use Example 2.4 of [8] to show that the closed subgroups of R given by Camina's construction are not in general arithmetically profinite subgroups of R.

Remark 3. Discussions with D. Segal and B. Klopsch show that every closed subgroup G of R which is in the image of the functor of fields of norms has Hausdorff dimension (for the definition see [1]) equal to zero. Indeed, the non-decreasing sequence of the set of breaks (s_i) of G satisfies $\sum(s_i - s_{i-1})/p^i = +\infty$, hence $\liminf i/s_i = 0$.

Remark 4. The closure of the torsion of R is different from R, since every automorphism with finite e (see the previous section) doesn't belong to the closure of the torsion of R (by the way, the closure of the group generated by the torsion of R coincides with R for $p > 2$). The same arguments as in the proof of Remark 1 show that every closed subgroup of R which is in the image of W and isn't a virtually-pro-p-cyclic group (i.e. it doesn't contain $\mathbb{Z} - p$ as a finite index subgroup) is inside the closure of the torsion of R. Hence there is an infinite chain of closed subgroups of R: $G_1 = R > G_2 > \dots$ such that all G_i are isomorphic to each other and each next is contained in the closure of the torsion of the previous one.

Corollary 2 (Lubotzky–Wilson). There is a pro-p-group with 2 generators which contains as a closed subgroup every countably based pro-p-group.

Proof. The group $R_{\mathbb{F}_p}$ does. $\square$

Problem. Given a free pro-p-group G with finite number of generators does there exist a Galois arithmetically profinite extension L of K, $|K : \mathbb{Q}_p| < +\infty$, such that $G(L/K)$ is isomorphic to G?

The affirmative answer will imply that for every finitely generated pro-p-group G there is a closed subgroup inside the group $R_{\mathbb{F}_q}$ isomorphic to G which comes via the functor of fields of norms from a Galois arithmetically profinite extension of local number fields.

We shall show in the next section that this is true for specific closed subgroups T of R which are different from pro-p-cyclic groups.

6. Subgroups $T[r]$ of the wild group.

For $m \geqslant 2$ define the following closed subgroups in the wild group $R = R_{\mathbb{F}_p}$

$$S_m = \Big\{\sum_{i\geqslant 0} a_i t^{1+mi} : a_0 = 1, a_i \in \mathbb{F}_p\Big\}.$$

For m relatively prime to p the group of principal units $1 + t^m\,\mathbb{F}_p[[t^m]]$ is uniquely m-divisible, therefore one can associate to an element $\sigma \in R$ considered as a wild automorphism of $\mathbb{F}_p((t^m))$ ($\sigma(t^m) = t^m f(t^m)$ with $f(t) \in 1 + t\mathbb{F}_p[[t]]$) an automorphism $\tau \in S_m$ considered as a wild automorphism of $\mathbb{F}_p((t))$: $\tau(t) = t\,\sqrt[m]{f(t^m)}$. Hence S_m is isomorphic to R and S_{mp^r} is isomorphic to S_{p^r}.

Fix $r \geqslant 1$, put $q = p^r$ and denote

$$T = T[r] = S_q, \qquad T_i = \{f(t) \in T : f(t) \in t + t^{1+qi}\,\mathbb{F}_p[[t]]\}.$$

To initiate the study of the structure of T we first state and prove five auxiliary lemmas. The reader can skip their proofs and look first at the main theorem at the end of this section.

We shall use the following notation: $j = \overline{\jmath}p^{n(j)}$ where $\overline{\jmath}$ is relatively prime to p.

Lemma 1. Fix s satisfying $1 \leqslant s \leqslant r$. Let $i > j \geqslant q^2$ and i be relatively prime to p. Let i_m, j_m satisfy the following conditions:
(i) $i_m \geqslant i$, $j_m \geqslant j - q$;
(ii) i_m *is relatively prime to* p;
(iii) $j_m \geqslant j$ *if* $i_m = i$; $qj_m + p^s i_m > qj + p^s i$ *if* $i_m > i$;
(iv) *if* $i_m + qj_m < j + qi$, *then* $i_m = r_m i + s_m q$ *with integers* $r_m \geqslant 1$, $s_m \geqslant 0$.

Let v_m, w_m, x_m, y_m, z_m be non-negative integers such that $v_m > 0$ if and only if $w_m > 0$, $x_m > 0$ if and only if $y_m > 0$, and $z_m > 0$ only if $x_m > 0$. Let q divide z_m if $z_m \leqslant qj$.

Then the equality

$$\sum(v_m i_m + w_m q j_m) + \sum(x_m j_m + y_m q i_m p^{n(j_m)} + z_m) = I + qj, \quad p^{s-1}i < I \leqslant p^s i, p^s | I$$

implies that
$I = p^s i$;
if $p^s < q$ *then up to renumbering terms* $v_1 = p^s, w_1 = 1$, $i_1 = i, j_1 = j$, *and* $v_m = w_m = 0$ *for* $m > 1$, $x_m = y_m = z_m = 0$ *for* $m \geqslant 1$;
if $p^s = q$, *then either up to renumbering terms* $v_1 = q, w_1 = 1$, $i_1 = i, j_1 = j$, *and* $v_m = w_m = 0$ *for* $m > 1$, $x_m = y_m = z_m = 0$ *for* $m \geqslant 1$ *or up to renumbering terms* $x_1 = q$,

$y_1 = 1$, $i_1 = i, j_1 = j$ (so j is relatively prime to p) and $v_m = w_m = z_m = 0$ for $m \geqslant 1$, $x_m = y_m = 0$ for $m > 1$.

Proof. Let not all v_m be zero. From (i) we deduce $i_m + qj_m \geqslant i + q(j-q)$ which is $> qj$ due to $i > q^2$. Then $x_m = y_m = z_m = 0$ for $m \geqslant 1$ and $\sum(v_m i_m + w_m q j_m) = I + qj$.

If all $v_m i_m + w_m q j_m$ are smaller than $j + qi$, then from (iv) we deduce $\sum v_m i_m = (\sum v_m r_m)i + (\sum v_m s_m)q$. Since i is relatively prime to p, p^s divides $\sum v_m r_m$ and therefore $\sum v_m i_m \geqslant p^s i$. Then $I + qj \geqslant p^s i + q(\sum w_m j_m)$. From (i) $2j_m \geqslant 2(j-q) > j$, therefore, up to renumbering, $w_1 = 1$, $v_m = w_m = 0$ for $m > 1$ and $v_1 i_1 + qj_1 = I + qj$. From (ii) we deduce that p^s divides v_1, so $v_1 i_1 + qj_1 \geqslant p^s i_1 + qj_1$, and the latter is $> p^s i + qj$ whenever $i_1 \neq i$ by (iii). Hence $i_1 = i$ and by (iii) $j_1 = j, v_1 = p^s, I = p^s i$.

If not all $v_m i_m + w_m q j_m$ are smaller than $j + qi$, then let, up to renumbering, $v_1 i_1 + w_1 q j_1 \geqslant j + qi$. From (i) and $i > j \geqslant q^2$ we deduce that $i_m + qj_m \geqslant i + q(j-q) > qj$, $v_m = w_m = 0$ for $m > 1$ and $v_1 i_1 + w_1 q j_1 = I + qj$. Now (ii) implies that $p^s | v_1$ and then $v_1 i_1 + w_1 q j_1 \geqslant p^s i_1 + qj_1$ which is $> p^s i + qj$ if $i_1 \neq i$ by (iii). Hence $i_1 = i$ and by (iii) $j_1 = j, v_1 = p^s, w_1 = 1, I = p^s i$.

Let all v_m be zero. From (i) and $i > j$ we deduce that $2qi_m > qi + qj$. Then, up to renumbering, $y_1 = 1$ and $x_m = y_m = z_m = 0$ for $m > 1$. Hence from $x_1 j_1 + q i_1 p^{n(j_1)} + z_1 = I + qj$ we derive that j_1 is relatively prime to p and $q | z_1$. Now from (ii) we deduce that p^s divides x_1. Hence $p^s i + qj \geqslant I + qj \geqslant p^s j_1 + q i_1$. Furthermore, $(p^s + q)i_1 \geqslant (p^s + q)i > p^s i + qj$ due to (i) and $i > j$; therefore $j_1 < i_1$. Now $p^s j_1 + q i_1 > p^s i_1 + q j_1$ if $p^s < q$, and $p^s i_1 + q j_1 > p^s i + qj$ if $i_1 \neq i$ by (iii). Therefore, $i_1 = i, p^s = q$ and by (iii) $j_1 = j, x_1 = q, y_1 = 1, z_1 = 0, I = qi$. $\square$

Lemma 2. Let $i > j$. Let $t(1 + a(t)) \in T_j$, $t(1 + b(t)) \in T_i$. Denote by $\alpha(t)$ and $\beta(t)$ the inverse series in T to $t(1 + a(t))$ and $t(1 + b(t))$ respectively. Then

$$\alpha(t) \equiv \frac{t}{1 + a(t)} \mod t^{q^2 j}\,\mathbb{F}_p[[t]], \qquad \beta(t) \equiv \frac{t}{1 + b(t)} \mod t^{q^2 i}\,\mathbb{F}_p[[t]]$$

and

$$[t(1 + a(t)), t(1 + b(t))] \equiv$$
$$t + \frac{t\big(a(t) - a(\beta(t))\big)}{(1 + a(t))} - \frac{t\big(b(t) - b(\alpha(t))\big)}{(1 + b(t))} \mod t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]].$$

Proof. Note that for $f_1(t) \in 1 + t^q\,\mathbb{F}_p[[t^q]]$, $f_2(t) \in 1 + t^l\,\mathbb{F}_p[[t]]$

$$(\triangledown) \qquad (tf_1(t)) \circ (tf_2(t)) \equiv tf_1(t)f_2(t) \mod t^{1+q(l+1)}\,\mathbb{F}_p[[t]].$$

Call $f_1(t), f_2(t)$ the reduced parts of $tf_1(t))$ and $tf_2(t))$. Then the previous formula shows modulo which degree the reduced part of the product of two elements in T is the product of their reduced parts.

Now, since $\alpha(t), \beta(t) \in t + t^{1+q}\,\mathbb{F}_p[[t^q]]$, we deduce that

$$\alpha(t) \equiv t/(1 + a(t)) \mod t^{1+q+q^2 j}\,\mathbb{F}_p[[t]], \qquad \beta(t) \equiv t/(1 + b(t)) \mod t^{1+q+q^2 i}\,\mathbb{F}_p[[t]],$$
$$(\alpha \circ \beta)(t) \equiv \alpha(t)/(1 + b(t)) \mod t^{1+q+q^2 i}\,\mathbb{F}_p[[t]]$$
$$(\beta \circ \alpha)(t) \equiv \beta(t)/(1 + a(t)) \equiv t/((1 + a(t))(1 + b(t))) \equiv (\alpha \circ \beta)(t) \mod t^{1+q+q^2 j}\,\mathbb{F}_p[[t]].$$

We have $[t(1+a(t)),t(1+b(t))]=t+c(\alpha(\beta(t)))$, where

$$\begin{aligned}c(t)&=t(1+a(t))\circ t(1+b(t))-t(1+b(t))\circ t(1+a(t))\\&=t(1+b(t))(a(t+tb(t))-a(t))-t(1+a(t))(b(t+ta(t))-b(t)).\end{aligned}$$

Let $a(t)=\sum_{k\geqslant j}a_kt^{qk}$ and let $b(t)=\sum_{l\geqslant i}b_lt^{ql}$. Then

$$t\big(1+b(t)\big)\big(a(t+tb(t))-a(t)\big)=t\bigg(1+\sum_{l\geqslant i}b_lt^{ql}\bigg)\sum_{k\geqslant j}a_kt^{qk}\bigg(\big(1+\sum_{l\geqslant i}b_lt^{q^2l}\big)^k-1\bigg).$$

Working modulo $t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]]$ and substituting a series in the previous expression, we can ignore terms of degree $\geqslant q^2j$ when substituting in t, terms of degree $\geqslant qj$ when substituting in the first and second sums, terms of degree $\geqslant j$ when substituting in the third sum. From the congruences for $\alpha(t),\beta(t)$ obtained above we get

$$\begin{aligned}&(t(1+b(t))(a(t+tb(t))-a(t))\circ\alpha(t)\circ\beta(t)\\&\equiv\big((t+tb(t))\circ\beta(t)\circ\alpha(t)\big)\cdot\big((a(t+tb(t))-a(t))\circ\beta(t)\big)\equiv\alpha(t)\cdot(a(t)-a(\beta(t)))\\&\equiv t/(1+a(t))\cdot(a(t)-a(\beta(t)))\mod t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]].\end{aligned}$$

Similarly,

$$t\big(1+a(t)\big)\big(b(t+ta(t))-b(t)\big)=t\bigg(1+\sum_{k\geqslant j}a_kt^{qk}\bigg)\sum_{l\geqslant i}b_lt^{ql}\bigg(\big(1+\sum_{k\geqslant j}a_kt^{q^2k}\big)^l-1\bigg).$$

Working modulo $t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]]$ and substituting a series in the previous expression, we can ignore terms of degree $\geqslant q^2i$ when substituting in t, terms of degree $\geqslant qi$ when substituting in the first and second sums, terms of degree $\geqslant i$ when substituting in the third sum. Then

$$\begin{aligned}&(t(1+a(t))(b(t+ta(t))-b(t))\circ\alpha(t)\circ\beta(t)\equiv\beta(t)\cdot(b(t+ta(t))-b(t))\circ\alpha(t)\\&\equiv t/(1+b(t))\cdot(b(t)-b(\alpha(t)))\mod t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]],\end{aligned}$$

which completes the proof. □

Lemma 3. Let $i>j\geqslant q^2$ and let i be relatively prime to p. Let $a_j=a,b\in\mathbb{F}_p^*$. Let $a_k\in\mathbb{F}_p$ and $a_k=0$ for k non-strictly between $j+1$ and qj which are not divisible by q.

Then

$$[t+\sum_{k\geqslant j}a_kt^{1+qk},t+bt^{1+qi}]$$

is congruent modulo $t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]]$ to

(a)

$$t+\sum_{j_m\geqslant j}c_mt^{1+q(v_mi+w_mqj_m)}+\sum_{j_m\geqslant j}d_mt^{1+q(x_mj_m+y_mqip^{n(j_m)}+z_m)}$$

where v_m,w_m,x_m,y_m,z_m together with $i_m=i$ and $j_m\geqslant j$ satisfy the conditions of Lemma 1 for every $s=1,\dots,r$;

(b)

$$t+\sum_{\nu\geqslant i} e_\nu t^{1+q(qj+\nu)} \mod t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]]$$

where the coefficients e_ν satisfy the following conditions:
(b1) *if $\nu+qj<j+qi$ and $e_\nu\neq 0$, then $\nu=s_\nu i+r_\nu q$ with integers $s_\nu\geqslant 1, r_\nu\geqslant 0$;*
(b2) *$e_{p^s i}=-iab\neq 0$ for $0\leqslant s<r$ and $e_{qi}=(j-i)ab$.*

Proof. Use Lemma 2 with $a(t)=\sum_{k\geqslant j} a_k t^{qk}$, $b(t)=bt^{qi}$. Let $\alpha(t)$ and $\beta(t)$ be the same as in Lemma 2; then $\alpha(t)=t+\sum_{k\geqslant j} c_k t^{1+qk}$, $c_j=-a$ by Lemma 2. We get

$$[t+\sum_{k\geqslant j} a_k t^{1+qk}, t+bt^{1+qi}]\equiv$$
$$t+\frac{t}{1+a(t)}(a(t)-a(\beta(t)))-\frac{t}{1+b(t)}(b(t)-b(\alpha(t))) \mod t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]].$$

Since $a(t)$ belongs to $\mathbb{F}_p[[t^q]]$, $a(\beta(t))\equiv a(t/(1+b(t)))\mod t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]]$ by Lemma 2. Now

$$[t+\sum_{k\geqslant j} a_k t^{1+qk}, t+bt^{1+qi}]\equiv$$
$$t+\frac{t}{1+\sum_{k\geqslant j} a_k t^{qk}}\left(\sum_{k\geqslant j} a_k t^{qk}\frac{(1+bt^{q^2 i})^k-1}{(1+bt^{q^2 i})^k}\right)-\frac{bt^{1+qi}}{1+bt^{qi}}\left(1-(1+\sum_{k\geqslant j} c_k t^{q^2 k})^i\right)$$
$$\equiv t+\frac{t}{1+\sum_{k\geqslant j} a_k t^{qk}}\left(\sum_{k\geqslant j} a_k t^{qk}\overline{k}bt^{q^2 i p^{n(k)}}\right)+\frac{bt^{1+qi}}{1+bt^{qi}}d(t) \mod t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]],$$

where

$$d(t)=\sum_{0<l_1+\cdots+l_m\leqslant i}\frac{i!}{l_1!\dots l_m!(i-l_1-\cdots-l_m)!}c_{k_1}^{l_1}\dots c_{k_m}^{l_m}t^{q^2(l_1k_1+\cdots+l_mk_m)}.$$

The first large term in the previous expression for the commutator consists of terms of degree $1+q(fk+f_1k_1+\cdots+f_mk_m)+q^2ip^{n(k)}$ with $k,k_1,\dots,k_m\geqslant j$, $f\geqslant 1$, $f_1,\dots,f_m\geqslant 0$. Due to the restrictions on a_k terms of degree $\leqslant 1+q^2(i+j)$ are of the type

$$1+qfj+q^2ip^{n(j)}+q(f_1k_1'+\cdots+f_mk_m')$$

with $f\geqslant 1$, $f_1,\dots,f_m\geqslant 0$, $q|k_1',\dots,k_m'\geqslant j/q$. This can be rewritten as $1+q(xj+yqip^{n(j)}+z)$ where $x,y>0$, $z\geqslant 0$, $q|z$.

The second large term in the previous expression for the commutator consists of terms of degree $1+fqi+q^2(l_1k_1+\cdots+l_mk_m)$ with $f\geqslant 1$, $k_1,\dots,k_m\geqslant j$, $l_1+\cdots+l_m>0$. We can rewrite this as $1+qj+q(fi+q(l_1k_1+\cdots+l_mk_m-j))$ or as $1+q(vi+qk)$ where $k\geqslant j$, $v>0$.

Now parts (a) and (b1) follow. To deduce part (b2) apply Lemma 1 to $i_m=i, j_m\geqslant j$ using part (a). Hence for $1\leqslant s<r$ the coefficient $e_{p^s i}$ comes from the second large expression in the three line formula; the coefficient e_{qi} comes from the both terms. The coefficient e_i is calculated directly. $\square$

Lemma 4. Let $i \geqslant j$. Let $a_k, b_l \in \mathbb{F}_p$. Then
(1) *the commutator $[t+\sum_{k\geqslant j} a_k t^{1+qk}, t+\sum_{l\geqslant i} b_l t^{1+ql}]$ belongs to T_{i+qj} and even to $T_{(q+1)i+1}$ if $i=j$;*
(2) *if $i > j(qp^{n(i)}-1)/(q-1)$ then*

$$[t+\sum_{k\geqslant j} a_k t^{1+qk}, t+bt^{1+qi}] \equiv t - \overline{i}a_j b t^{1+q(i+qp^{n(i)}j)} \mod T_{i+qp^{n(i)}j+1}.$$

Proof. Apply Lemma 2 to calculate the first commutator. It is congruent modulo $T_{q(i+j)+1}$ to

$$t + \frac{t}{1+\sum_{k\geqslant j} a_k t^{qk}} \sum_{k\geqslant j} a_k (t^{qk} - \beta(t)^{qk}) - \frac{t}{1+\sum_{l\geqslant i} b_l t^{ql}} \sum_{l\geqslant i} b_l (t^{ql} - \alpha(t)^{ql}),$$

where $\alpha(t), \beta(t)$ have the same meaning as in Lemma 2. By the same lemma

$$\beta(t) \equiv t - b_i t^{1+qi} \mod t^{1+qi+q}\,\mathbb{F}_p[[t]], \qquad \alpha(t) \equiv t - a_j t^{1+qj} \mod t^{1+qj+q}\,\mathbb{F}_p[[t]],$$

so

$$\alpha(t)^{ql} \equiv t^{ql} - \overline{l}a_j t^{ql+q^2 jp^{n(l)}} \mod t^{ql+q^2jp^{n(l)}+q}\,\mathbb{F}_p[[t]]$$

and

$$\beta(t)^{qk} \equiv t^{qk} - \overline{k}b_i t^{qk+q^2 ip^{n(k)}} \mod t^{qk+q^2ip^{n(k)}+q}\,\mathbb{F}_p[[t]].$$

Since $qj+q+q^2ip^{n(k)}, qi+q+q^2jp^{n(l)} \geqslant q(i+qj+1)$, the first commutator is congruent modulo T_{i+qj+1} to

$$t + a_j b_i \overline{j} t^{1+qj+q^2ip^{n(j)}} - a_j b_i \overline{i} t^{1+qi+q^2jp^{n(j)}}$$

and so belongs to T_{i+qj} and even to T_{i+qi+1} if $i=j$.

To deduce (2) use the first formula in this proof. From the previous calculations

$$\frac{t}{1+\sum_{k\geqslant j} a_k t^{qk}} \sum_{k\geqslant j} a_k (t^{qk} - \beta(t)^{qk}) \in t^{1+qj+q^2 i}\,\mathbb{F}_p[[t]]$$

and

$$\frac{bt}{1+bt^{qi}}(t^{qi} - \alpha(t)^{qi}) \equiv \overline{i}a_j b t^{1+qi+q^2jp^{n(i)}} \mod t^{1+q+qi+q^2jp^{n(i)}}\,\mathbb{F}_p[[t]].$$

Thus, to deduce (2) it remains to use $qj+q^2i \geqslant q+qi+q^2jp^{n(i)}$ iff $(q-1)i > j(qp^{n(i)}-1)$. □

A natural number l is said to be associated to a subgroup H of T if $T_l \leqslant T_{l+1}H$.

Lemma 5. Let H be a non-trivial closed normal subgroup of an open subgroup G of T. Then
(1) *for every $n \geqslant 0$ there is l_n such that all $p^n l \geqslant l_n$ with l relatively prime to p are associated to H.*
(2) *For every $a \in \mathbb{F}_p^*$ and every $j \geqslant \max(l_0, \dots, l_{r-1})$ relatively prime to p there is a series $t + \sum_{k\geqslant j} a_k t^{1+qk}$ in H, $a_j = a$, satisfying the following property: if $j+1 \leqslant k \leqslant qj+q^2$, $q \not| k$ then $a_k = 0$.*

Proof. The group G contains some T_k. Fix $n \geqslant 0$. Take any $j = p^m\overline{\jmath}$ with $(\overline{\jmath}, p) = 1$ such that some element $f(t) = t + at^{1+qp^m\overline{\jmath}} + \dots$ belongs to H. Then $[f(t), T_k] \leqslant H$. From Lemma 4, (2) we deduce that for $u \geqslant u_0$ relatively prime to p the element $[f(t), t + bt^{1+qp^n u}] = t - abut^{1+qp^n u+q^2p^{n+m}\overline{\jmath}} + \dots$ belongs to H. Hence $p^n(u + qp^m\overline{\jmath})$ is associated to H and there is l_n such that all $p^n l \geqslant l_n$ with l relatively prime to p are associated to H. We work with the wild group over $\mathbb{F}_p$, so if $p^n l \geqslant l_n$ with l relatively prime to p, then for every $a \in \mathbb{F}_p^*$ there is a series $t + at^{1+qp^n l} + \dots \in H$: just use the relation $h(t) \circ h(t) = t + 2et^{1+qk} + \dots$ for a series $h(t) = t + et^{1+qk} + \dots$.

Let $j \geqslant \max(l_0, \dots, l_{r-1})$ be relatively prime to p. Assume that for $j' \geqslant j$ there is a series $f_{j'}(t) = t + \sum_{k \geqslant j} b_k t^{1+qk} \in H$ with $b_k = a$, $b_k = 0$ for k between $j+1$ and j' not divisible by q. If q doesn't divide $j'+1$, then since $j'+1 \geqslant \max(l_0, \dots, l_{r-1})$ there is a series $g(t) = t + \sum_{k \geqslant j'+1} c_k t^{1+qk} \in H$ with $c_{j'+1} = -b_{j'+1}$. Now by $(\triangledown)$ in the proof of Lemma 2 we deduce that the series $f_{j'+1}(t) = f_{j'}(t) \circ g(t) = t + \sum_{k \geqslant j} d_k t^{1+qk} \in H$ satisfies the property: $d_k = a$, $d_k = 0$ for k between $j+1$ and $j'+1$ not divisible by q. Induction implies (2). $\square$

Theorem. Let $p > 2$.
(1) *If $\sigma \in T_i \setminus T_{i+1}$ then $\sigma^p \in T_{pi} \setminus T_{pi+1}$; the intersection of T with the closure of the torsion of R is trivial.*
(2) *$[T_i, T_i] \leqslant T_{(q+1)i+1}$ and the group $T_i/T_{(q+1)i}$ is abelian of exponent pq.*
(3) *$[T,T]T^p > T_{q+2}$; the number of generators of T is at most $q+1$.*
(4) *T is not a p-adic Lie group.*
(5) *A non-trivial normal closed sugroup of an open subgroup of T is open.*

Proof.

(1) For $\alpha \in F = \mathbb{F}_p((t))$ one has $v_F((\sigma - 1)\alpha) \geqslant v_F(\alpha) + i(\sigma)$ with equality when $v_F(\alpha)$ is relatively prime to p. Therefore

$$i(\sigma^p) = v_F((\sigma^p - 1)(t)) - 1 = v_F((\sigma - 1)^p(t)) - 1 \geqslant pi(\sigma),$$

hence $R_n^p \leqslant R_{np}$ and $i(\sigma^p) = v_F((\sigma - 1)^p(t)) - 1 = pi(\sigma)$ for $i(\sigma) = qi$.

(2) From part (1) of Lemma 4 $[T_i, T_i] \leqslant T_{(q+1)i+1}$. Then (1) implies that $T_i/T_{(q+1)i}$ is abelian of exponent pq.

(3) From Lemma 4, (2) we know that if $i > j$ and i is relatively prime to p, then $[t + at^{1+qj}, t + bt^{1+qi}] = t - iabt^{1+qi+q^2j} + \dots$. Therefore $T_l \leqslant T_{l+1}[T,T]$ for all $l \geqslant q+2$ relatively prime to p. By (1) $T_{pi} \leqslant T_{pi+1}T^p$ and the assertion follows.

(4) If T were a p-adic Lie group, then by [6], Th. 9.34 it would contain an open subgroup G which is a uniformly powerful pro-p-group, so in particular $G^p = \{g^p : g \in G\}$ would be a subgroup of $[G,G]$, see [6], Prop. 2.6. However, the subgroup $[G,G]$ contains some elements $t + t^{1+qi} + \dots$ with i relatively prime to p which are obviously not in G^p. Alternatively, the group T doesn't contain an open subgroup of finite rank (and so it isn't

p-adic Lie by [6], Cor. 9.35), since the cardinality of $T_i/[T_i,T_i]T_i^p$ tends to infinity when i tends to infinity.

(5) The proof of this assertion uses Lemma 1, Lemma 3, Lemma 5 and the congruence $(\triangledown)$ in the proof of Lemma 2. Let $j \geqslant \max(q^2, l_0, \dots, l_{r-1}) + q$ where l_m are defined in Lemma 5 (1). Let $i > j$, and let $i, j, i-j$ be relatively prime to p. Let $T_i \leqslant G$. The main purpose of the following arguments is to find in H a product of several commutators which is equal to $t + o_{qi}t^{1+q^2i+q^2j} + \dots$, $o_{qi} \neq 0$, and deduce that $q(i+j)$ is associated to H.

In the course of the proof we shall pick up elements $\theta_{j'}(t) = t + at^{1+qj'} + \dots \in H$, $a \neq 0$, as in Lemma 5 (2) applied to $j' \geqslant j - q$. Then $qj' + q^2 \geqslant qj$ and therefore the coefficient of t^{1+qk} in $\theta_{j'}(t)$ for $k < qj$, $q \not| k$ is zero.

Let $\theta_j(t) = t + at^{1+qj} + \dots \in H$, $a \neq 0$, be as in Lemma 5 (2). Then for $b \neq 0$ Lemma 3 shows that

$$[\theta_j(t), t + bt^{1+qi}] \equiv t + \sum_{\nu \geqslant i} e_\nu t^{1+q(qj+\nu)}$$
$$\equiv t + \sum_{j_m \geqslant j} c_m t^{1+q(v_m i + w_m q j_m)} + \sum_{j_m \geqslant j} d_m t^{1+q(x_m j_m + y_m q i p^{n(j_m)} + z_m)}$$

modulo $t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]]$, where in particular the following properties are satisfied:

$\flat$ if $\nu + qj < j + qi$ and $e_\nu \neq 0$, then $\nu = r_\nu i + s_\nu q$ with integers $r_\nu \geqslant 1, s_\nu \geqslant 0$;
for $0 \leqslant s \leqslant r$ $\quad \sharp(s) \quad$ $e_{p^s i} \neq 0$.

From Lemma 3 it follows that for every $e_i \in \mathbb{F}_p^*$ there is an appropriate b such that the commutator's second term is $e_i t^{1+q(qj+i)}$. Denote the commutator by $\omega_0(i, j, i+qj, e_i)$.

Let $\theta_{j-p}(t) = t + at^{1+q(j-p)} + \dots \in H$, $a \neq 0$, be as in Lemma 5 applied to $j-p$ instead of j. Then Lemma 3 shows that

$$[\theta_{j-p}(t), t + ct^{1+q(i+qp)}] \equiv t + \sum_{\nu \geqslant i+qp} e'_\nu t^{1+q(qj+\nu-qp)}$$
$$\equiv t + \sum_{j_m \geqslant j-p} c'_m t^{1+q(v_m(i+qp)+w_m q j_m)} + \sum_{j_m \geqslant j-p} d'_m t^{1+q(x_m j_m + y_m q(i+qp) p^{n(j_m)} + z_m)}$$

modulo $t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]]$ with the standard properties. If $e'_\nu \neq 0$ and $\nu + q(j-p) < j + qi$, then $\nu + q(j-p) < j - p + q(i+qp)$, so from $\flat$ for $i+qp, j-p$ we get $\nu = r_\nu(i+qp) + s_\nu q$ and $\nu - qp = r_\nu i + q(s_\nu + p(r_\nu - 1))$ with integers $r_\nu \geqslant 1, s_\nu \geqslant 0$.

The congruence $(\triangledown)$ in the proof of Lemma 2 and the trivial inequality $q(q^2j + qi) > q^2(i+j)$ shows that the reduced part of the product in T of $[\theta_j(t), t+bt^{1+qi}]$ and $[\theta_{j-p}(t), t+ct^{1+q(i+qp)}]$ modulo $t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]]$ is given by the usual product of their reduced parts. Hence for an appropriate $c \in \mathbb{F}_p$

$$[\theta_j(t), t + bt^{1+qi}] \circ [\theta_{j-p}(t), t + ct^{1+q(i+qp)}] \equiv t + \sum_{\nu > i} f_\nu t^{1+q(qj+\nu)} \mod t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]].$$

From Lemma 1 applied to $(i_m, j_m) \in \{(i, \geqslant j)\} \cup \{(i+qp, \geqslant j-p)\}$ and the natural observation

$$j + qi > \nu_1 + qj + \nu_2 + qj \Longrightarrow \nu_1 + qj + \nu_2 + qj = (r_{\nu_1} + r_{\nu_2})i + (s_{\nu_1} + s_{\nu_2} + j)q + qj$$

we deduce that f_ν satisfy $\flat$ and $\sharp(1)-\sharp(r)$.

Lemma 1 shows that f_ν for ν divisible by p and satisfying $i<\nu<pi$ are zero. Let f_{ν_0} be the first non-zero coefficient in terms of degree $>1+q^2j+qi$ and $<1+qj+q^2i$ in the last congruence. Since $f_{pi}\neq 0$, we get $\nu_0=r_{\nu_0}i+s_{\nu_0}q\leqslant pi$. Assume that $\nu_0<pi$, then ν_0 is relatively prime to p. Consider the product

$$[\theta_j(t),t+bt^{1+qi}]\circ[\theta_{j-p}(t),t+ct^{1+q(i+qp)}]\circ\omega_0(r_{\nu_0}i+s_{\nu_0}q,j,\nu_0+qj,-f_{\nu_0}).$$

Note that if $\nu+qj<j+qi$, then $\nu+qj<j+q\nu_0$ and $r_\nu\nu_0+s_\nu q=r_\nu r_{\nu_0}i+q(r_\nu s_{\nu_0}+s_\nu)$ with integers $r_\nu r_{\nu_0}\geqslant 1, r_\nu s_{\nu_0}+s_\nu\geqslant 0$. Lemma 1 applied to $(i,\geqslant j),(i+qp,\geqslant j-p),(\nu_0,\geqslant j)$ and relation $(\triangledown)$ in the proof of Lemma 2 imply that the latter product is congruent modulo $t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]]$ to $t+\sum_{\nu>i_0}g_\nu t^{1+q(qj+\nu)}$ and g_ν satisfy $\flat$ and $\sharp(1)-\sharp(r)$.

Repeating, if necessary, we get a product of several commutators, call it $\omega_1(i,j,pi+qj,h_{pi})$, such that

$$\omega_1(i,j,pi+qj,h_{pi})\equiv t+\sum_{\nu\geqslant pi}h_\nu t^{1+q(qj+\nu)}\mod t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]]$$

where h_ν satisfy $\flat$ and $\sharp(1)-\sharp(r)$.

Proceed by induction using Lemma 1, Lemma 3 and the relation $(\triangledown)$ in the proof of Lemma 2. Assume that for $1\leqslant n\leqslant s<r$ we have already constructed elements $\omega_n(i,j,p^ni+qj,k_{p^ni})$ in H as products of appropriate commutators of the type discussed in Lemma 3 so that in particular

$$\omega_n(i,j,p^ni+qj,k_{p^ni})\equiv t+\sum_{\nu\geqslant p^ni}k_\nu t^{1+q(qj+\nu)}\mod t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]]$$

where k_ν satisfy $\flat$ and $\sharp(n)-\sharp(r)$.

To eliminate the term $t+k_{p^s}t^{1+q(qj+p^si)}$ for $s<r$ multiply by $\omega_s(i+q,j-p^s,p^si+qj,-k_{p^s})$ and apply Lemma 3, Lemma 1 for $s+1,\dots,r$.

To eliminate the term $l_\nu t^{1+q(qj+\nu)}$ where $p^si<\nu<p^{s+1}i$, $\nu=p^n\overline{\nu}$ with $\overline{\nu}$ being relatively prime to p first deduce from Lemma 3, Lemma 1 and $(\triangledown)$ that $0\leqslant n\leqslant s$ and hence $\overline{\nu}>i$. Then use Lemma 3 and Lemma 1 for $s+1,\dots,r$ and either multiply by $\omega_n(\overline{\nu},j,\nu+qj,-l_\nu)$ if $\nu+qj\geqslant j+qi$ or by $\omega_n(r_\nu p^{-n}i+s_\nu qp^{-n},j,\nu+qj,-l_\nu)$ if $\nu+qj<j+qi$, $\nu=r_\nu i+s_\nu q$. Note that $(r_\nu p^{-n},p)=1$ by Lemma 1.

Each time the coefficients of the new product of commutators satisfy $\flat$ and $\sharp(s+1)-\sharp(r)$. Hence in H we get the element

$$\omega_{s+1}(i,j,p^{s+1}i+qj,m_{p^{s+1}i})\equiv t+\sum_{\nu\geqslant p^{s+1}i}m_\nu t^{1+q(qj+\nu)}\mod t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]]$$

where m_ν satisfy $\flat$ and $\sharp(s+1)-\sharp(r)$.

Thus, by induction we produce

$$\omega_r(i,j,qi+qj,o_{qi})\equiv t+\sum_{\nu\geqslant qi}o_\nu t^{1+q(qj+\nu)}\mod t^{1+q^2(i+j)+q}\,\mathbb{F}_p[[t]]$$

with $o_{qi}\neq 0$. We conclude that $q(i+j)$ is associated to H.

Keeping in mind the restrictions on i,j at the beginning of this part and Lemma 5 (1) we deduce that all sufficiently large l belong to H. Since H is closed, T_l is contained in H for sufficiently large l and H is open. $\square$

Remark. Remark 4 in section 5 and the property (1) of the theorem show that no closed non-pro-p-cyclic subgroups of T are in the image of the functor W. Section 4 implies that pro-p-cyclic subgroups of T come from arithmetically profinite $\mathbb{Z}_p$-extensions in characteristic 0 only.

7. *Extensions of local number fields with the Galois group T.*

Recall that a Galois extension L/F is called deeply ramified if the set of its upper ramification breaks is unbounded. The theory of deeply ramified extensions of local fields and its applications in Kummer's theory of abelian varieties was developed in [5] by J. Coates and R. Greenberg. For various examples of deeply ramified extensions and their relations with arithmetically profinite extensions see [8].

Theorem. Let $r \geqslant 2$ and $q = p^r$. Let F be an unramified extension of $\mathbb{Q}_p$ of degree $\geqslant q$.
(1) *There is a Galois extension L of F which is deeply ramified and $G(L/F)$ is isomorphic to $T[r]$.*
(2) *The extension L/F is arithmetically profinite.*
(3) *If $F \subset K \subset E \subset L$ with finite K/F and infinite Galois E/K, then $G(E/K)$ is not a p-adic Lie group.*

Proof. (1) According to Shafarevich's theorem [26] the pro-p-part $G(F(p)/F)$ of the absolute Galois group of F is a free pro-p-group with $|F : \mathbb{Q}_p| + 1$ generators.

By part (3) of the theorem in the previous section $T = T[r]$ is isomorphic to the quotient of $G(F(p)/F)$, so there is a Galois extension L/F with the Galois group isomorphic to T.

Denote by F_i the fixed field of the subgroup in $G(L/F)$ corresponding to T_i. Let F^{unp} be the maximal unramified p-extension of F.

For a finite Galois extension E/K and an automorphism $\sigma \neq 1$ of E/K denote by $t_{E/K}(\sigma)$ the maximal rational number x such that σ doesn't belong to the upper ramification group $G(E/K)^v$ for every $v > x$. Denote by $u(E/K) = \max\{t_{E/K}(\sigma) : \sigma \in G(E/K), \sigma \neq 1\}$ its maximal upper ramification break (see for instance [9], Ch. III, sect. 5). Following Sen [25] we say that an abelian extension M/K is non-small if $u(M/K) > pe(K)/(p-1)$ where $e(K)$ is the absolute ramification index of K. We are going to apply Lemma 3.7 in [25] to certain subgroups G_n of T. We shall check that all conditions of Lemma 3.7 in [25] are satisfied.

Due to (1), (2) of the theorem in the previous section T_1/T_q decomposes into the direct product of the cyclic group of order q generated by $t + t^{1+q}$, the cyclic group of order q generated by $t + t^{1+2q}$ and an abelian group. Therefore the Galois group of the extension $F_q/F_q \cap F^{\mathrm{unp}}$ decomposes into the direct product of the cyclic group of order q and an abelian group. Since the field $F_q \cap F^{\mathrm{unp}}$ is absolutely unramified, local class field theory implies that $F_q/F_q \cap F^{\mathrm{unp}}$ is non-small. Put $I = G(L/L \cap F^{\mathrm{unp}})$. Then I as a normal closed subgroup of T is of finite index in T by (5) of the theorem in section 6. Put $G_n = T_{p^{n-1}} \cap I$, $G = G_1$. Since T_{p^n}/T_{qp^n} is abelian by part (2)

of the theorem in section 6, G_n/G_{n+2} is abelian for every $n \geqslant 1$. The abelian field extension $F_q(L \cap F^{\mathrm{unp}})/L \cap F^{\mathrm{unp}}$ is non-small, since $F_q/F_q \cap F^{\mathrm{unp}}$ is non-small. Finally, from part (1) of the theorem in the previous section we deduce that G_n coincides with $\{\sigma \in G : \sigma^p \in G_{n+1}\}$. Thus, all conditions of Lemma 3.7 in [25] are satisfied. Therefore by Lemma 3.7 in [25] $u(F_{p^{n+1}}(L \cap F^{\mathrm{unp}})/L \cap F^{\mathrm{unp}}) = u(F_{p^n}(L \cap F^{\mathrm{unp}})/L \cap F^{\mathrm{unp}}) + e(F)$ for $p^n \geqslant q$. In particular, the extension L/F is deeply ramified.

(2) The extension L/F is arithmetically profinite: every subgroup $G(L/F)^x$ of T is non-trivial by (1) and closed normal, therefore it is open of finite index by property (5) of the theorem in section 6.

(3) Normal extensions E of K in L are either finite over K or coincide with L and therefore $G(E/K)$ is not p-adic Lie by part (4) of the theorem in section 6. $\square$

8. *Problem of Coates and Greenberg.*

The following problem was stated in [5], p. 144:

> *Is it true that for every finite extension K of $\mathbb{Q}_p$ there exists a deeply ramified Galois p-extension M of K such that that no subfield M' of M is an infinitely ramified Galois extension of a finite extension Q of $\mathbb{Q}_p$ with $G(M'/Q)$ being a p-adic Lie group ?*

This problem is related to Fontaine–Mazur's conjecture on unramified Galois representations of a number field and its generalization by Boston [2]. Note that results of [23] and [25] (the proof of Serre's conjecture) imply that every infinite p-adic Lie extension (i.e. the Galois group being p-adic Lie) in characteristic 0 with finite residue field extension is deeply ramified, and moreover, arithmetically profinite.

Using the theorem of section 7 one can provide the affirmative answer on Coates–Greenberg's problem by taking the normal closure of KL over K as M.

Indeed, the extension M/K is deeply ramified. If φ is the Frobenius automorphism of KF over K and ϕ is its lifting to the algebraic closure of $\mathbb{Q}_p$, then M is the compositum of a finite number of fields $K\phi^n(L)$, $0 \leqslant n < |KF : K|$. Each $\phi^n(L)/F$ is a normal extension with the Galois group isomorphic to T.

Let R_1 and R_2 be infinite Galois extensions of a finite extension R of $\mathbb{Q}_p$, and let $G(R_1/R)$ be isomorphic to T. We are going to show that if $G(R_1R_2/R)$ has an open subgroup which has an infinite p-adic Lie quotient, then $G(R_2/R)$ has an open subgroup which has an infinite p-adic Lie quotient. Applying that to M and $K\phi^n(L)$ we then deduce that if there is a subfield M' of M which is a Galois extension of a finite extension Q of $\mathbb{Q}_p$ with $G(M'/Q)$ being infinite p-adic Lie, then T has an open subgroup which has an infinite p-adic Lie quotient, which contradicts the theorem in section 7.

So let there be a subfield N of R_1R_2 which is a Galois extension of a finite extension O of R with $G(N/O)$ being infinite p-adic Lie. We can assume that O/R is a Galois extension. Let $R_1 \not\subset R_2$. Then $G(R_1/R_1 \cap R_2)$ is a normal non-trivial closed subgroup

of $G(R_1/R)$, so $R_1/R_1 \cap R_2$ is infinite. Therefore the group $G(R_1/R_1 \cap OR)$ is a normal non-trivial closed subgroup of $G(R_1/R)$, so it and $G(OR_1/OR)$ are isomorphic to an open subgroup of T. Due to the properties of the group T described in the theorem of section 7 the extension $N \cap OR_1/OR$ is of finite degree and so is $N \cap OR_1/O$. Therefore $N/N \cap OR_1$ is an infinite p-adic Lie extension and so $G(NR_1/OR_1)$ is an infinite p-adic Lie quotient of an open subgroup $G(R_1R_2/OR_1)$ of $G(R_1R_2/R_1)$. We conclude that $G(R_2/R)$ has an open subgroup which has an infinite p-adic Lie quotient, as required.

Remark. The affirmative answer on the problem stated in section 4 will imply that every finitely generated hereditary just infinite pro-p-group (every non-trivial normal closed subgroup of an open subgroup is open) can be realized as the Galois group of an arithmetically profinite extension of a local number field, therefore providing a collection of extensions L/F answering Coates–Greenberg's problem.

References

[1] Barnea Y., Shalev, A.: Hausdorff dimension, pro-p-groups, and Kac–Moody algebras. Trans. of the AMS **349**, 5073–5091(1997)

[2] Boston, N.: Some cases of the Fontaine–Mazur conjecture. II. Algebraic Number Theory Archives, 129(1998), http://www.dpmms.cam.ac.uk/ Algebraic-Number-Theory/

[3] Camina, R.: Subgroups of the Nottingham group. J. Algebra **196**, 101–113(1997)

[4] Cartwright, D.: Pro-p-groups and Lie algebras over local fields of characteristic p. Ph. D. Thesis, QMW, London 1997

[5] Coates, J., Greenberg, R.: Kummer theory for abelian varieties over local fields. Invent. Math. **124**, 129–174(1996)

[6] Dixon, J.D., du Sautoy, M.P.F.,Mann, A., Segal, D.: Analytic pro-p-groups. LMS Lect. Notes Series **157**, 2nd edit., Cambridge Univ. Press, Cambridge 1999

[7] du Sautoy, M.P.F.: Pro-p-Groups. Preprint, Cambridge 1997

[8] Fesenko, I.: On deeply ramified extensions. Journal of the LMS (2), **57**, 325–335(1998)

[9] Fesenko, I., Vostokov, S.: Local Fields and Their Extensions. AMS, Providence, R.I. 1993

[10] Fontaine, J.–M.: Un résultat de Sen sur les automorphismes de corps locaux. Séminaire Delange-Pisot-Poitou, Paris (1969–1970) exposé 6

[11] Fontaine, J.–M., Winteneberger, J.–P.: Le "corps des normes" de certaines extensions algébriques de corps locaux. C. R. Acad. Sc. Paris, **288**, 367–370(1979)

[12] Iwasawa, K.: On solvable extensions of algebraic number fields. Ann. Math. **58**, 548–572(1953)

[13] Johnson, D.L.: The group of formal power series under substitution. J. Austral. Math. Soc. (Series A) **45**, 298–302(1988)

[14] Klopsch, B.: Normal subgroups and automorphisms of substitution groups of formal power series. Preprint, Oxford 1997

[15] Laubie, F.: Extensions de Lie et groupes d'automorphismes de corps locaux. Comp. Math. **67**, 165–189(1988)

[16] Laubie, F., Saine, M.: Ramification of automorphisms of $k((t))$. J. Number Theory **63**, 143–145(1997)

[17] Laubie, F.: Sur la ramification des extensions de Lie. Comp. Math. **98**, 253–262(1985)

[18] Leedham–Green, C.R., Plesken, W., Klaas, G.: Linear pro-p-groups of finite width. Preprint, Aachen–London 1997

[19] Li, H.-Ch.: p-adic periodic points and Sen's theorem. J. Number Theory **56**, 309–318(1996)

[20] Lubin, J.: Non-archimedean dynamical systems. Comp. Math. **94**, 321–346(1994)

[21] Lubotzky, A., Shalev, A.: On some Λ-analytic pro-p-groups. Israel J. Math. **85**, 307–337(1994)

[22] Lubotzky, A., Wilson, J.S.: An embedding theorem for profinite groups. Arch. Math. **42**, 397–399(1984)

[23] Maus, E.: Über die Verteilung der Grundverzweigungszahlen von wild verzweigeten Erweiterungen ƀ-adishcher Zahlkörper. J. reine und angew. Math. **257**, 47–79(1972)

[24] Sen, Sh.: On automorphisms of local fields. Ann. Math. **90**, 33–46(1969)

[25] Sen, Sh.: Ramification in p-adic Lie extensions. Invent. Math. **17**, 44–50(1972)

[26] Shafarevich, I. R.: On p-extensions. Mat. Sb., Nov. Ser. **20**, 351–363(1947)

[27] Wintenberger, J.–P.: Automorphismes et extensions galoisiennes de corps locaux. Thèse de 3 cycle, Grenoble 1978

[28] Wintenberger, J.–P.: Extensions de Lie et groupes d'automorphismes des corps locaux de caractéristique p. C. R. Acad. Sc. **288** série A, 477-479(1979)

[29] Wintenberger, J.–P.: Extensions abéliennes et groupes d'automorphismes des corps locaux. C. R. Acad. Sc. **290** série A, 201–203(1980)

[30] Wintenberger, J.–P.: Le corps des normes de certaines extensions infinies des corps locaux; applications. Ann. Sci. E.N.S., 4 série **16**, 59–89(1983)

[31] York, I. O.: The group of formal power series under substitution. Ph. D. Thesis, Nottingham 1990

[32] Shalev, A.: Lie methods in the theory of pro-p groups. In New horizons in pro-p groups, ed. du Sautoy, M., Segal, D. and Shalev, A., Progress in Math., Birkhauser, 2000

[33] du Sautoy, M., Fesenko, I.: Where the wild groups are: ramification groups and the Nottingham group. In New horizons in pro-p groups, ed. du Sautoy, M., Segal, D. and Shalev, A., Progress in Math., Birkhauser, 2000

Department of Mathematics
University of Nottingham
NG7 2RD Nottingham England