Annals of Mathematics, **137** (1993), 639–670

Finitely generated groups, p-adic analytic groups and Poincaré series

By MARCUS P.F. DU SAUTOY

Introduction

Let G be a group and denote by $a_n(G)$ the number of subgroups of index n in G. We shall only be interested in groups for which $a_n(G)$ is finite for each $n \geq 1$. To each prime p and group G we can then associate the following Poincaré series:

$$\zeta_{G,p}(s) = \sum_{n=0}^{\infty} a_{p^n}(G) p^{-ns}.$$

In this article we are concerned with the following question:

Question. For which groups G and primes p can $\zeta_{G,p}(s)$ be written as a rational function in p^{-s}?

This is equivalent to the coefficients $a_{p^n}(G)$ satisfing a linear recurrence relation with constant coefficients for sufficiently large n.

These Poincaré series were first studied in the case when G is a finitely generated, torsion-free nilpotent group in a paper by Grunewald, Segal and Smith [GSSm]. There the authors established that, for such a group, $\zeta_{G,p}(s)$ is a rational function in p^{-s}. In that setting the functions $\zeta_{G,p}(s)$ are the local factors associated with the Dirichlet series

$$\zeta_G(s) = \sum_{n=1}^{\infty} a_n(G) n^{-s}$$

and $\zeta_G(s)$ is equal to the product of these local factors. However this "Euler product" decomposition does not appear to generalize to the case of non-nilpotent groups.

In this article we show how integrals with respect to the Haar measure on a pro-p-group can be used to deduce the rationality of our Poincaré series from some very general finiteness conditions on a group G.

This generalizes the philosophy introduced by Igusa ([I1], [I2]). He showed how to express Poincaré series associated with p-adic varieties as integrals with respect to the additive Haar measure on $\mathbb{Z}_p$. Applying techniques from

geometry, in particular Hironaka's resolution of singularities, one can evaluate a limited class of such integrals as rational functions in p^{-s}. More recently Denef and van den Dries ([D1], [D2] and [DvdD]) have applied results from logic, profiting from the flexibility of the concept "definable", greatly to enlarge the class of integrals amenable to Igusa's method. In subsection 1.1 we describe the class of integrals considered by Denef and van den Dries.

In subsection 1.2 we consider integrals of the following form, defined with respect to the Haar measure $\mathrm{d}\mu$ on a pro-p-group G:

$$Z(h,k,\mathcal{M},s) = \int_{\mathcal{M}} p^{-sh(g_1,\ldots,g_r)-k(g_1,\ldots,g_r)}\mathrm{d}\mu;$$

where $\mathcal{M} \subseteq G \times \cdots \times G = G^{(r)}$ and $h,k : G^{(r)} \to \mathbb{Z}$. We define a twosort language $\mathcal{L}_G$ associated with the class of pro-p-groups—the first sort ranges over elements of the group G and the second sort over the p-adic integers allowing us to define the natural action of $\mathbb{Z}_p$ on a pro-p-group. We also have a twoplace predicate, which defines the lower p-series $P_i(G)$ on G, where $P_1(G) = G$ and $P_{i+1}(G) = \overline{P_i(G)^p[P_i(G),G]}$. The key technical result of this article concerns the case where G is a *uniform* pro-p-group—that is, a finitely generated pro-p-group with the property that

(i) G/G^p (or G/G^4 if $p = 2$) is abelian, and

(ii) $|G : P_2(G)| = |P_i(G) : P_{i+1}(G)|$ for each $i \geq 1$.

THEOREM A. *Let G be a uniform pro-p-group and $\mathcal{M}$, h and k be as above. If $\mathcal{M}$ is definable in $\mathcal{L}_G$ and the functions h and k are constructed from definable functions in $\mathcal{L}_G$, then $Z(h,k,\mathcal{M},s)$ is rational in p^{-s}.*

A more detailed statement of this result can be found in Theorem 1.17. The key ingredient in the proof of this theorem is one half of Lazard's solution to the p-adic version of Hilbert's fifth problem. He showed how to define a natural manifold structure on a uniform pro-p-group G (or *p-saturable* group in the terminology of his 1965 paper [L]) with respect to which the group operations are analytic; i.e., such a group G is a p-adic analytic group. We show here that the natural action of $\mathbb{Z}_p$ on G is also defined by analytic functions. Using this structure on G, we show how to translate the definable group-theoretic integrals $Z(h,k,\mathcal{M},s)$ into the integrals of subsection 1.1 considered by Denef and van den Dries.

In Section 2 we use the rationality results of Section 1 to prove the following theorem:

THEOREM B. *Let G be a compact p-adic analytic group. Then $\zeta_{G,p}(s)$ is a rational function in p^{-s}.*

In fact our techniques allow us to deal with the Dirichlet series counting *all* subgroups associated with a compact p-adic analytic group:

THEOREM C. *Let G be a compact p-adic analytic group. Then there exist an integer N and rational functions $\Phi_n(X)$ for each divisor n of N such that*

$$\zeta_G(s) = \sum_{n|N} n^{-s}\Phi_n(p^{-s}).$$

(Note that, although in the context of profinite groups it is more natural to count just open subgroups, in the situation of Theorems B and C all subgroups of finite index are in fact open.)

We prove also that Theorem B is the best possible one in the case of a pro-p-group G—namely that the rationality of $\zeta_{G,p}(s)$ implies that G is a p-adic analytic group.

The proofs of Theorems B and C rely on the second half of Lazard's solution to the p-adic version of Hilbert's fifth problem—that is, every compact p-adic analytic group contains an open uniform subgroup. We begin in subsection 2.1 by showing how to express the Poincaré series, counting subgroups in a uniform pro-p-group as one of the definable group-theoretic integrals of subsection 1.2. In subsection 2.2 we then show how to extend these integrals to count subgroups in finite extensions of our uniform pro-p-groups. In subsection 2.3 we prove rationality results for variants of our Poincaré series where we count only *normal subgroups* (subsection 2.3.1), *r-generated subgroups* (subsection 2.3.2) and finally the number of *conjugacy classes of subgroups* (subsection 2.3.3).

In Section 3 we apply the results of Section 2 to prove rationality results for the Poincaré series associated with finitely generated groups satisfying some very general finiteness conditions. The philosophy behind the proofs in that section is to identify a compact p-adic analytic group, whose subgroups are in one-to-one correspondence with subgroups we wish to count in our finitely generated group.

The pro-p-completion of an abstract group gives us access to counting only subnormal subgroups of p-power index. In particular, using Lubotzky and Mann's criterion in terms of polynomial subgroup growth for a pro-p-group to be analytic (see [LuM2]), we prove the next theorem:

THEOREM D. *Let Γ be a finitely generated group, p a prime and denote by $a_n^{\mathrm{s}}(\Gamma)$ the number of subnormal subgroups of index n in Γ. If $a_{p^n}^{\mathrm{s}}(\Gamma)$ grows at most polynomially with respect to p^n, then*

$$\zeta_{\Gamma,p}^{\mathrm{s}}(s) = \sum_{n\in\mathbb{N}} a_{p^n}^{\mathrm{s}}(\Gamma)p^{-ns}$$

is rational in p^{-s}.

However, under suitable finiteness conditions on a group Γ, we can identify a subgroup Γ_0 of finite index, all of whose subgroups of p-power index are subnormal. By extending the pro-p-completion of this group Γ_0 by a finite group, we can construct a compact p-adic analytic group G having open subgroups corresponding to all subgroups of p-power index in Γ. This approach allows us to prove the following theorem (the *upper p-rank* of Γ is the supremum of the ranks of all p-subgroups of finite quotients of Γ):

THEOREM E. *Let p be a prime and let Γ be a finitely generated group with finite upper p-rank. Then $\zeta_{\Gamma,p}(s)$ is rational in p^{-s}.*

An announcement of some of the results contained in this article appeared in [duS1].

In a sequel [duS2] we apply the philosophy of Section 3 to the problem of counting congruence subgroups in arithmetic groups. As a corollary to that we mention the following result:

THEOREM F. *Let Γ be an arithmetic lattice inside $G = \mathrm{SL}_n$, where $n \geq 3$. Then $\zeta_{\Gamma,p}(s)$ is rational in p^{-s} for all primes p.*

The proof relies on various ingredients, including Guralnick's classification of subgroups of prime-power index in simple groups (cf. [Gu]) and the work of Shorey and Tijdeman on exponential diophantine equations (cf. [ShT]). Note that in Theorem F, $\zeta_{\Gamma,p}(s) = 1$ for almost all primes p.

Notation. The notation in subsection 1.1 is borrowed from the earlier paper by [DvdD]. We have consistently used boldface to denote a tuple (or vector) of elements.

$\langle \mathbf{i} \rangle = i_1 + \cdots + i_M$, where $\mathbf{i} = (i_1, \ldots, i_M) \in \mathbb{N}^M$.

$\mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_M^{i_M}$, where $\mathbf{X} = (X_1, \ldots, X_M)$ are commuting indeterminates and $\mathbf{i} = (i_1, \ldots, i_M) \in \mathbb{N}^M$.

$\boldsymbol{\lambda}^{\mathbf{n}} = \lambda_1^{n_1} \cdots \lambda_M^{n_M}$, where $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_M) \in \mathbb{Z}_p^M$ and $\mathbf{n} = (n_1, \ldots, n_M) \in \mathbb{N}^M$.

$H \leq_p G$ if H is a subgroup of p-power index in G.

$H \trianglelefteq_p G$ if H is a normal subgroup of p-power index in G.

$G^{(r)} = G \times \cdots \times G$, the direct product of r copies of a group G.

$\mathcal{H}$ denotes sets of subgroups.

$\mathcal{M}$ denotes sets of good bases for subgroups.

$\mathcal{N}$ denotes sets of bases for subgroups.

$\mathrm{M}_{r \times d}$ denotes the ring of matrices.

1. Rationality of definable integrals

1.1. *Definable p-adic integrals.* For $r \in \mathbb{Q}_p$, $|r|$ denotes the normalized absolute value $p^{-v(r)}$, where $v(r) = \mathrm{ord}_p(r)$. We denote by ν the additive Haar measure on $\mathbb{Z}_p$, so normalized that $\nu(\mathbb{Z}_p) = 1$, and also (by abuse of notation) the product measure on free $\mathbb{Z}_p$-modules of the form $\mathbb{Z}_p^M$.

With each pair of functions $f_1 : \mathbb{Z}_p^M \to \mathbb{Q}_p$, $f_2 : \mathbb{Z}_p^M \to \mathbb{Q}_p$ and the subset $S \subseteq \mathbb{Z}_p^M$ we associate the following function:

$$I(f_1, f_2, S, s) = \int_S |f_1(\mathbf{x})|^s |f_2(\mathbf{x})| \mathrm{d}\nu.$$

(Here s denotes a complex variable and $\mathbf{x} = (x_1, \ldots, x_M)$ ranges over S.)

This integral generalizes Igusa's local zeta function (cf. [I1]). In this section we describe the class of integrals evaluated by Denef and van den Dries as rational in p^{-s}.

Definition 1.1. Let $\mathbf{X} = (X_1, \ldots, X_M)$ be M commuting indeterminates and let $\mathbb{Q}_p[[\mathbf{X}]]$ denote the set of formal power series

$$\sum_{\mathbf{i} \in \mathbb{N}^M} a_{\mathbf{i}} X_1^{i_1} \cdots X_M^{i_M}$$

in the commuting indeterminates, where $a_{\mathbf{i}} \in \mathbb{Q}_p$. We define the following subsets of $\mathbb{Q}_p[[\mathbf{X}]]$:

(i) $\mathbb{Z}_p[[\mathbf{X}]]$ denotes the set of power series $\sum a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$ with $a_{\mathbf{i}} \in \mathbb{Z}_p$ for all $\mathbf{i} \in \mathbb{N}^m$;

(ii) $\mathbb{Q}_p\{\mathbf{X}\}$ consists of all formal power series $\sum a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$ such that $|a_{\mathbf{i}}| \to 0$ as $\langle \mathbf{i} \rangle \to \infty$;

(iii) $\mathbb{Z}_p\{\mathbf{X}\} = \mathbb{Z}_p[[\mathbf{X}]] \cap \mathbb{Q}_p\{\mathbf{X}\}$.

(Here $\langle \mathbf{i} \rangle = i_1 + \cdots + i_M$, where $\mathbf{i} = (i_1, \ldots, i_M)$.)

Definition 1.2. Let V be a nonempty open subset of $\mathbb{Z}_p^M$ and let $f : \mathbb{Z}_p^M \to \mathbb{Z}_p$ be a function from V into $\mathbb{Z}_p$. We say that f is *analytic* at $\mathbf{y} \in V$ if there exist a formal power series $F(\mathbf{X}) \in \mathbb{Z}_p\{\mathbf{X}\}$ and $h \in \mathbb{N}$ such that $f(\mathbf{y} + p^h \mathbf{x}) = F(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}_p^M$. We say that f is *analytic* on V if it is analytic at each point of V.

We shall need the following two lemmas concerning analytic functions.

LEMMA 1.3. *Suppose that $f_1, \ldots, f_N : \mathbb{Z}_p^M \to \mathbb{Z}_p$ and $g : \mathbb{Z}_p^N \to \mathbb{Z}_p$ are analytic functions on $\mathbb{Z}_p^M$ and $\mathbb{Z}_p^N$, respectively. Then $g \circ \mathbf{f} : \mathbb{Z}_p^M \to \mathbb{Z}_p$ is analytic on $\mathbb{Z}_p^M$.*

Proof. See [DxduSMS], Ch. 9, Lemma 9.4. □

LEMMA 1.4. *Suppose that* $F(\mathbf{X}) = \sum_{\mathbf{i}\in\mathbb{N}^M} a_{\mathbf{i}} X_1^{i_1} \cdots X_M^{i_M}$ *converges on some open subset* U *of* $\mathbb{Z}_p^M$. *Then there exists* n *such that* $p^{n(\mathbf{i})} a_{\mathbf{i}} \in \mathbb{Z}_p$.

Proof. See [DxduSMS], Ch. 7, Lemma 7.18. □

Definition 1.5. (i) We define the function $D : \mathbb{Z}_p^2 \to \mathbb{Z}_p$ by

$$D(x,y) = \begin{cases} x/y & \text{if } |x| \le |y| \text{ and } y \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

(ii) For $n > 0$ we define P_n to be the set of nonzero n^{th} powers in $\mathbb{Z}_p$.

We define now the language considered in [DvdD].

Definition 1.6. Let $\mathcal{L}_{an}^D$ be the language with logical symbols $=$, $\neg$, $\vee$, $\wedge$, a countable number of variables X_i and

(i) an m-place operation symbol F for each $F(\mathbf{X}) \in \mathbb{Z}_p\{\mathbf{X}\}$, $m \ge 0$;

(ii) a binary operation symbol D; and

(iii) a unary relation symbol P_n for each $n > 0$.

Note that if $m = 0$, then $F(\mathbf{X})$ defines constant terms in our language for each element of $\mathbb{Z}_p$.

We refer the reader to [DvdD], §0, for a self-contained account of the notions from logic that we shall use. In particular we have the concept of a formula in $\mathcal{L}_{an}^D$ and its interpretation in an $\mathcal{L}_{an}^D$ structure. For our purposes we shall only be interested in the structure $\mathbb{Z}_p$ and then the following shows how to interpret a formula in this structure:

Definition 1.7. Each formula $\phi(X_1, \ldots, X_M)$ in the language $\mathcal{L}_{an}^D$ defines a subset

$$M_\phi = \{\mathbf{x} \in \mathbb{Z}_p^M \mid \phi(\mathbf{x}) \text{ is true in } \mathbb{Z}_p\},$$

where we interpret

(i) each $F \in \mathbb{Z}_p\{\mathbf{X}\}$ as the function $f : \mathbb{Z}_p^M \to \mathbb{Z}_p$ defined by $f(\mathbf{x}) = F(\mathbf{x})$;

(ii) the binary operation symbol D as the function in Definition 1.5, and

(iii) $P_n(x)$ to be true if $x \in P_n$, where P_n is the subset in Definition 1.5.

We call such a subset M_ϕ *definable* (in $\mathcal{L}_{an}^D$). A function $f : V \to \mathbb{Z}_p$ is called *definable* if its graph is a definable subset. We shall call $I(f_1, f_2, S, s)$ a *definable integral* if $f_1 : \mathbb{Z}_p^M \to \mathbb{Q}_p$ and $f_2 : \mathbb{Z}_p^M \to \mathbb{Q}_p$ are definable functions and S is a definable subset of $\mathbb{Z}_p^M$.

THEOREM 1.8. *Suppose that* $I(f_1, f_2, S, s)$ *is a definable integral. Then*

(i) S *is measurable, and*

(ii) $I(f_1, f_2, S, s)$ *is a rational function in* p^{-s}, *which can be written as a polynomial in* p^{-s} *with rational coefficients, divided by a product of factors of*

the form $(1 - p^{-a-sb})$ *with* $a, b \in \mathbb{Z}$. *Moreover each pole of* $I(f_1, f_2, S, s)$ *has multiplicity at most* M, *where* M *is the number of variables in* $I(f_1, f_2, S, s)$.

The reader should consult [DvdD] and [D3] for a proof of this theorem. However let us mention the essential steps in the proof.

(i) $\mathbb{Z}_p$ admits quantifier elimination in the language $\mathcal{L}_{an}^D$. This result, due to Denef and van den Dries, extends Macintyre's quantifier elimination for the algebraic theory of $\mathbb{Z}_p$ (see [M]). It allows us to decompose the definable integral into a finite sum of integrals over sets defined by formulae without quantifiers.

(ii) We then apply a p-adic analogue of Hironaka's rectilinearization theorem to eliminate occurrences of the function D.

(iii) These much simpler integrals can then be evaluated (à la Igusa) by the use of a version of Hironaka's embedded resolution of singularities. In [vdD], van den Dries outlines a proof of Theorem 1.8 without using any resolution of singularities.

In the next section we shall define a language for the theory of pro-p-groups, which we shall interpret in the language $\mathcal{L}_{an}^D$. To do this we need the following two lemmas:

LEMMA 1.9. *Let* $f : \mathbb{Z}_p^M \to \mathbb{Z}_p$ *be an analytic function. Then* f *is a definable function in* $\mathcal{L}_{an}^D$.

Proof. For each $\mathbf{a} \in \mathbb{Z}_p^M$ there exist a formal power series

$$F(\mathbf{X}) = \sum_{\mathbf{i} \in \mathbb{N}^M} a_{\mathbf{i}} X_1^{i_1} \cdots X_M^{i_M} \in \mathbb{Q}_p[[\mathbf{X}]]$$

and $h \in \mathbb{N}$ such that if $\mathbf{x} \in \mathbf{a} + p^h \mathbb{Z}_p^M$, then $f(\mathbf{x}) = F(\mathbf{x} - \mathbf{a})$. By Lemma 1.4 there exists $n \in \mathbb{N}$ such that $p^{\langle \mathbf{i} \rangle n} a_{\mathbf{i}} \in \mathbb{Z}_p$ for all $\mathbf{i} \in \mathbb{N}^M$. (Note that since $f(\mathbf{a}) \in \mathbb{Z}_p$, this ensures that $a_{\mathbf{0}} \in \mathbb{Z}_p$.) Let

$$G(\mathbf{X}) = \sum_{\mathbf{i} \in \mathbb{N}^M} p^{\langle \mathbf{i} \rangle n} a_{\mathbf{i}} X_1^{i_1} \cdots X_M^{i_M} \in \mathbb{Z}_p[[\mathbf{X}]]$$

and $N = \max(n+1, h)$. If $\mathbf{x} \in \mathbf{a} + p^N \mathbb{Z}_p^M$, then $f(\mathbf{x}) = G(D(\mathbf{x} - \mathbf{a}, p^{n+1}))$. Since $\{\mathbf{a} + p^N \mathbb{Z}_p^M \mid \mathbf{a} \in \mathbb{Z}_p^M\}$ is an open cover of the compact space $\mathbb{Z}_p^M$, there exists a finite cover $\{\mathbf{a}_i + p_i^N \mathbb{Z}_p^M\}$ on which f is given by a definable function $G_i(D(\mathbf{x} - \mathbf{a}_i, p^{n_i+1}))$. Since each of the open subsets is definable, this implies that f is definable. □

LEMMA 1.10. *The twoplace predicate defined by* $v(x) \geq v(y)$ *is definable in* $\mathcal{L}_{an}^D$.

Proof. An application of Hensel's lemma implies that for all $x, y \in \mathbb{Z}_p$

$$v(x) \geq v(y) \text{ if and only if } \begin{cases} x = 0 \text{ or } y^2 + px^2 \in P_2 & \text{if } p \neq 2, \\ x = 0 \text{ or } y^2 + 8x^2 \in P_2 & \text{if } p = 2. \end{cases}$$ □

1.2. *Definable group-theoretic integrals.* In this subsection we define a filtered group-theoretic language $\mathcal{L}_G$ and a class of integrals over the Haar measure of a group that can be evaluated as rational functions. Although there is not much content beyond translating these integrals into the integrals considered in the previous section, we do provide a more convenient setting for the proofs to come in the latter half of this article.

Let G be a pro-p-group. Then G admits a natural action of $\mathbb{Z}_p$ as detailed in the following:

Definition 1.11. Let $\lambda \in \mathbb{Z}_p$ and $g \in G$. We define

$$g^{\lambda} = \lim_{n \to \infty} g^{a_n},$$

where (a_n) is a sequence of rational integers with $\lim_{n\to\infty} a_n = \lambda$. (It is a straightforward exercise to show that this is well defined.)

The following series of (topologically) characteristic subgroups associated with a pro-p-group G will be of importance to us:

Definition 1.12. Let G be a pro-p-group. We define the *lower p-series* in G to be $\{P_i(G) \mid i \geq 1\}$, where $P_1(G) = G$ and $P_{i+1}(G) = \overline{P_i(G)^p[P_i(G), G]}$. (Here $\overline{H}$ denotes the topological closure of the set H in G.) Define $\omega : G \to \mathbb{N} \cup \{\infty\}$ by $\omega(g) = n$ if $g \in P_n(G) \setminus P_{n+1}(G)$ and $\omega(1) = \infty$.

Note that $P_2(G)$ is the Frattini subgroup of G. If G is finitely generated (topologically), then the minimum number of topological generators for G, denoted by $d(G)$, is $\dim_{\mathbb{F}_p} G/P_2(G)$. We now associate a twosort language to the pro-p-group G. (A twosort language is a language with two distinct sets of variables called *sorts*. We must then specify on which sort a function or predicate in the language is defined. An interpretation of such a language entails naming two domains over which the two sorts range.)

Definition 1.13. Let $\mathcal{L}_G$ be the language having two sorts x and λ. We have constant symbols in the sort x, for each element of the pro-p-group, together with a binary relation symbol $x|y$ on the sort $x \times x$. We have the following function symbols, which all define elements in the sort x:

(i) a binary function symbol $x.y$ on the sort $x \times x$;

(ii) a unary function symbol x^{-1} on the sort x;

(iii) a binary function symbol x^{λ} on the sort $x \times \lambda$;

(iv) a class of unary function symbols ϕ on x.

We construe a pro-p-group G as an $\mathcal{L}_G$ structure by allowing the sort x to range over G and the sort λ to range over $\mathbb{Z}_p$. The interpretation of the function symbols is clear, apart from the class in (iv), which we shall interpret as specific automorphisms of our group G. The symbol $x|y$ will be interpreted as the relation $\omega(x) \geq \omega(y)$.

Definition 1.14. We shall call a subset $\mathcal{M} \subseteq G \times \cdots \times G = G^{(r)}$ *definable* if there exists a formula $\psi(x_1, \ldots, x_r)$ in $\mathcal{L}_G$ with r free variables of sort x such that

$$\mathcal{M} = \{(g_1, \ldots, g_r) \mid \psi(g_1, \ldots, g_r) \text{ is true in } G\}.$$

A function is called *definable* if its graph is definable.

Let μ be the normalized Haar measure on G and (by abuse of the notation) the product measure on $G \times \cdots \times G = G^{(r)}$. Let $\mathcal{M}$ be a definable subset of $G^{(r)}$ and h_i and k_j be definable functions ($i = 1, \ldots, m$ and $j = 1, \ldots, n$). We shall consider the following integrals

$$Z(h, k, \mathcal{M}, s) = \int_{\mathcal{M}} p^{-sh(g_1,\ldots,g_r)-k(g_1,\ldots,g_r)} \mathrm{d}\mu,$$

where $h : \mathcal{M} \to \mathbb{Z}$ and $k : \mathcal{M} \to \mathbb{Z}$ are defined by

$$h(g_1, \ldots, g_r) = \delta_1 \omega(h_1(g_1, \ldots, g_r)) + \cdots + \delta_m \omega(h_m(g_1, \ldots, g_r)),$$
$$k(g_1, \ldots, g_r) = \epsilon_1 \omega(k_1(g_1, \ldots, g_r)) + \cdots + \epsilon_n \omega(k_n(g_1, \ldots, g_r)),$$

and $\delta_i, \epsilon_j \in \mathbb{Z}$. We describe a class of pro-p-groups for which this function is a rational function in p^{-s}.

Definition 1.15. A pro-p-group G is *uniformly powerful*, or just *uniform*, if

(i) G is finitely generated;
(ii) G is powerful—that is, G/G^p (or G/G^4 if $p = 2$) is abelian; and
(iii) for all $i \geq 1$,

$$|P_i(G) : P_{i+1}(G)| = |G : P_2(G)|.$$

Lazard called such groups *p-saturable*; for a detailed account, see [DxduSMS], Ch. 4. These groups were the key to his characterization of compact topological groups with the underlying structure of a p-adic analytic group—the p-adic version of Hilbert's fifth problem (see [L] or [DxduSMS], Ch. 9).

THEOREM 1.16. *A compact topological group has the structure of a p-adic analytic group if and only if it contains an open normal subgroup that is a uniformly powerful pro-p-group.*

We use Lazard's work on the analytic structure of uniformly powerful pro-p-groups to prove the following:

THEOREM 1.17. *Let G be a uniformly powerful pro-p-group and let $\bar{\phi}_1, \ldots, \bar{\phi}_t$ be automorphisms of G. Suppose that $\mathcal{M}$ is a definable subset and h_i and k_j are definable functions ($i = 1, \ldots, m$ and $j = 1, \ldots, n$) in $\mathcal{L}_G$, where the function symbols $\phi_1, \ldots, \phi_t$ are interpreted as the automorphisms $\bar{\phi}_1, \ldots, \bar{\phi}_t$. Then $Z(h, k, \mathcal{M}, s)$ is a rational function in p^{-s} (where $h : \mathcal{M} \to \mathbb{Z}$ and $k : \mathcal{M} \to \mathbb{Z}$ are defined above).*

We begin the proof with the following:

THEOREM 1.18. *Let G be a uniformly powerful pro-p-group with $d(G) = d$. Let $\{x_1, \ldots, x_d\}$ be a (topological) generating set for G.*

(i) *For each $x \in G$ there exist unique $\lambda_1, \ldots, \lambda_d \in \mathbb{Z}_p$ with the property that*

$$x = x_1^{\lambda_1} \cdots x_d^{\lambda_d} = \mathbf{x}(\boldsymbol{\lambda}), \text{ say.}$$

(ii) *The function $f : \mathbb{Z}_p^d \times \mathbb{Z}_p^d \to \mathbb{Z}_p^d$ defined by*

$$\mathbf{x}(\boldsymbol{\lambda})(\mathbf{x}(\boldsymbol{\mu}))^{-1} = \mathbf{x}(f(\boldsymbol{\lambda}, \boldsymbol{\mu}))$$

is an analytic function.

(iii) *Let ϕ be an automorphism of G. The function $\Phi : \mathbb{Z}_p^d \to \mathbb{Z}_p^d$ defined by*

$$\mathbf{x}(\boldsymbol{\lambda})^{\phi} = \mathbf{x}(\Phi(\boldsymbol{\lambda}))$$

is an analytic function.

(iv) *If $x = \mathbf{x}(\boldsymbol{\lambda}) \in G$, then $\omega(x) = \min\{v(\lambda_i) + 1 \mid i = 1, \ldots, d\}$.*

Part (i) provides us with a global coordinate system with respect to which, by part (ii), the group operation is analytic. Thus the group has the structure of a p-adic analytic group. The proof of (i) follows by succesively approximating the element x with respect to the filtration $\{P_i(G) \mid i \geq 1\}$. We shall apply a similar argument when we consider subgroups of G. Part (ii) is proved by using the completion of the group ring $\mathbb{Z}_p[G]$ with respect to a filtration induced from the lower p-series on G. Part (iii) follows from the fact that the analytic structure on the uniform pro-p-group G defined in (i) is the unique analytic structure that makes G into an analytic group. Part (iv) is a consequence of the fact that, for a uniform pro-p-group G, the p^{th} power map $x \mapsto x^p$ induces an isomorphism

$$f_i : P_i(G)/P_{i+1}(G) \to P_{i+1}(G)/P_{i+2}(G),$$

where if $x = \mathbf{x}(\boldsymbol{\lambda}) \in P_i(G)$, then $f_i(\mathbf{x}(\boldsymbol{\lambda}))P_{i+1}(G) = \mathbf{x}(p\boldsymbol{\lambda})P_{i+2}(G)$.

For proofs of these statements we refer the reader to Lazard's original paper [L] or to Chapters 4 and 8-10 of [DxduSMS].

This theorem is the key to interpreting filtered group-theoretic statements in the language $\mathcal{L}_{an}^{D}$ described in subsection 1.1. We shall also need the following lemma:

LEMMA 1.19. *The function* $g : \mathbb{Z}_p^d \times \mathbb{Z}_p \to \mathbb{Z}_p^d$ *defined by*

$$\mathbf{x}(\boldsymbol{\lambda})^{\mu} = \mathbf{x}(g(\boldsymbol{\lambda}, \mu))$$

is an analytic function on $\mathbb{Z}_p^d \times \mathbb{Z}_p$.

Proof. By part (ii) of Theorem 1.18, for each $i = 1, \ldots, d$, there exist $a_{i\mathbf{mn}} \in \mathbb{Q}_p$ such that for all $\boldsymbol{\lambda}, \boldsymbol{\mu} \in \mathbb{Z}_p^d$

$$f_i(\boldsymbol{\lambda}, \boldsymbol{\mu}) = \sum_{(\mathbf{m},\mathbf{n}) \in \mathbb{N}^{2d}} a_{i\mathbf{mn}} \lambda_1^{m_1} \cdots \lambda_d^{m_d} \cdot \mu_1^{n_1} \cdots \mu_d^{n_d}.$$

By Lemma 7.19 of [DxduSMS] there exists $k \in \mathbb{N}$ such that for each $i = 1, \ldots, d$ and $(\mathbf{m}, \mathbf{n}) \in \mathbb{N}^{2d}$

$$a'_{i\mathbf{mn}} = p^{k(\langle \mathbf{m} \rangle + \langle \mathbf{n} \rangle)} a_{i\mathbf{mn}} \in \mathbb{Z}_p.$$

We shall prove that the function $g : p^{k+2}\mathbb{Z}_p^d \times p\mathbb{Z}_p \to \mathbb{Z}_p^d$ is analytic. By Lemma 10.2 and the proof of Proposition 10.1 of [DxduSMS] there exist power series

$$\psi_{ij}(\mathbf{X}) = \sum_{\mathbf{n} \in \mathbb{N}^d} c_{ij\mathbf{n}} X_1^{n_1} \cdots X_d^{n_d} \in \mathbb{Z}_p[[\mathbf{X}]]$$

for $i = 1, \ldots, d$ and $j \geq 1$, with the property that $c_{ij\mathbf{n}} = 0$ for $\langle \mathbf{n} \rangle < j$ and, for each $\boldsymbol{\lambda} \in p^{k+2}\mathbb{Z}_p^d$ and $\mu \in \mathbb{Z}_p$,

$$g_i(\boldsymbol{\lambda}, \mu) = \sum_{j=1}^{\infty} \binom{\mu}{j} \psi_{ij}(p^{-k}\boldsymbol{\lambda}).$$

Define $\nu_{jm} \in \mathbb{Q}$ by $\binom{\mu}{j} = \sum_{m \in \mathbb{N}} \nu_{jm} \mu^m$. Suppose now that $\boldsymbol{\lambda} \in p^{k+2}\mathbb{Z}_p^d$ and $\mu \in p\mathbb{Z}_p$. Then

$$g_i(\boldsymbol{\lambda}, \mu) = \sum_{j=1}^{\infty} \left(\sum_{m \in \mathbb{N}} \left(\sum_{\mathbf{n} \in \mathbb{N}^d} c_{ij\mathbf{n}} \nu_{jm} \mu^m (p^{-k}\boldsymbol{\lambda})^{\mathbf{n}} \right) \right).$$

If we can prove that

$$\lim_{(j,m,\mathbf{n}) \in \mathbb{N}^{d+2}} |c_{ij\mathbf{n}} \nu_{jm} \mu^m (p^{-k}\boldsymbol{\lambda})^{\mathbf{n}}| = 0, \tag{1.1}$$

then by Proposition 7.11 of [DxduSMS]

$$g_i(\boldsymbol{\lambda}, \mu) = \sum_{(m,\mathbf{n})\in\mathbb{N}^{d+1}} c'_{m\mathbf{n}}\mu^m\boldsymbol{\lambda}^{\mathbf{n}},$$

where $c'_{m\mathbf{n}} = \sum_{j=1}^{\infty} c_{ij\mathbf{n}}\nu_{jm}p^{-\langle\mathbf{n}\rangle k}$; i.e., g is analytic on $p^{(k+2)}\mathbb{Z}_p \times p\mathbb{Z}_p$.

To prove equation (1.1) note that $|\nu_{jm}| \leq |j!| \leq p^{(j-1)/(p-1)}$ by Lemma 7.21 of [DxduSMS]. So for all j and m

$$|c_{ij\mathbf{n}}\nu_{jm}\mu^m(p^{-k}\boldsymbol{\lambda})^{\mathbf{n}}| \leq p^{(j-1)/(p-1)} \cdot p^{-2\langle\mathbf{n}\rangle}.$$

Since $c_{ij\mathbf{n}} = 0$ for $j > \langle\mathbf{n}\rangle$, we have $\lim_{\langle\mathbf{n}\rangle\to\infty} |c_{ij\mathbf{n}}\nu_{jm}\mu^m(p^{-k}\boldsymbol{\lambda})^{\mathbf{n}}| = 0$ uniformly in j and m. It suffices now to prove that, for $\langle\mathbf{n}\rangle$ fixed,

$$\lim_{j+m\to\infty} |c_{ij\mathbf{n}}\nu_{jm}\mu^m(p^{-k}\boldsymbol{\lambda})^{\mathbf{n}}| = 0.$$

But this follows from the fact that $c_{ij\mathbf{n}} = 0$ for $j > \langle\mathbf{n}\rangle$ and

$$|c_{ij\mathbf{n}}\nu_{jm}\mu^m(p^{-k}\boldsymbol{\lambda})^{\mathbf{n}}| \leq \theta p^{-m}$$

for some constant θ. Thus equation (1.1) holds.

If $a \in \mathbb{Z}$, then $g_a : \mathbb{Z}_p^d \to \mathbb{Z}_p^d$, defined by

$$\mathbf{x}(\boldsymbol{\lambda})^a = \mathbf{x}(g_a(\boldsymbol{\lambda})),$$

is analytic. We finish the proof of our lemma by proving that, for each $a \in \mathbb{Z}$, $g : \mathbb{Z}_p^d \times (a + p^{k+3}\mathbb{Z}_p) \to \mathbb{Z}_p^d$ is analytic. Now

$$\mathbf{x}(\boldsymbol{\lambda})^{a+p^{k+3}\mu} = \mathbf{x}(g_a(\boldsymbol{\lambda})) \cdot \mathbf{x}(g_{p^{k+2}}(\boldsymbol{\lambda}))^{p\mu}. \tag{1.2}$$

But $g_{p^{k+2}}(\boldsymbol{\lambda}) \in p^{k+2}\mathbb{Z}_p^d$. Since compositions of analytic functions are analytic, equation (1.2) implies that g is analytic on $\mathbb{Z}_p^d \times (a + p^{k+3}\mathbb{Z}_p)$ for all $a \in \mathbb{Z}$, i.e., g is an analytic function on $\mathbb{Z}_p^d \times \mathbb{Z}_p$. □

LEMMA 1.20. *Let G be a uniformly powerful pro-p-group with $d(G) = d$ and let $\{x_1, \ldots, x_d\}$ be a topological generating set for G. Define*

$$\phi : \mathrm{M}_{r\times d}(\mathbb{Z}_p) \to G \times \cdots \times G = G^{(r)}$$

by $\phi(M) = (\mathbf{x}(\mathbf{m}_1), \ldots, \mathbf{x}(\mathbf{m}_r))$, where $\mathbf{m}_i$ denotes the i^{th} row of the matrix $M \in \mathrm{M}_{r\times d}(\mathbb{Z}_p)$.

(i) *ϕ is a homeomorphism.*

(ii) *If $X \subseteq G^{(r)}$ is definable in $\mathcal{L}_G$, then $\phi^{-1}(X)$ is definable in $\mathcal{L}_{an}^D$.*

(iii) *X is a measurable subset if and only if $\phi^{-1}(X)$ is a measurable subset of $\mathrm{M}_{r\times d}(\mathbb{Z}_p)$. In this case, $\mu(X) = \nu(\phi^{-1}(X))$.*

Proof. Part (i) follows from Theorem 4.9 of [DxduSMS]. Part (ii) is a consequence of Theorem 1.18 and Lemma 1.19 together with Lemmas 1.9 and

1.10. We prove part (iii) as follows: The additive Haar measure ν on $\mathbb{Z}_p^d$ defines a measure on G. The measure ν induces a measure on G/G_{n+1}, which coincides with the measure induced by μ on G/G_{n+1}. By Bourbaki's Integration VII ([B], §1.6), this implies that the measures ν and μ coincide on G. From this part (iii) follows. □

Proof of Theorem 1.17. Fix a topological generating set for G. Let $S \subseteq \mathrm{M}_{r\times d}(\mathbb{Z}_p)$ be the set of matrices M such that

$$(\mathbf{x}(\mathbf{m}_1), \ldots, \mathbf{x}(\mathbf{m}_r)) \in \mathcal{M},$$

where $\mathbf{m}_i$ denotes the i^{th} row of M. Then, by part (ii) of Lemma 1.20, S is definable. We define the functions $H_i : S \to \mathbb{Z}_p^d$ and $K_j : S \to \mathbb{Z}_p^d$ $(i = 1, \ldots, m$ and $j = 1, \ldots, n)$ by

$$\mathbf{x}(H_i(M)) = h_i(\mathbf{x}(\mathbf{m}_1), \ldots, \mathbf{x}(\mathbf{m}_r)),$$
$$\mathbf{x}(K_j(M)) = k_j(\mathbf{x}(\mathbf{m}_1), \ldots, \mathbf{x}(\mathbf{m}_r)).$$

By part (ii) of Lemma 1.20 the functions H_i and K_j $(i = 1, \ldots, m$ and $j = 1, \ldots, n)$ are definable.

Define for each $j = 1, \ldots, d$

$$A_j = \{\mathbf{a} \in \mathbb{Z}_p^d \mid v(a_j) < v(a_i) \text{ for } 1 \le i < j, v(a_j) \le v(a_i) \text{ for } j \le i \le d\}.$$

Then $\{A_j \mid j = 1, \ldots, d\}$ is a partition of $\mathbb{Z}_p^d$ into definable subsets. Define $\theta : \mathbb{Z}_p^d \to \mathbb{Z}_p$ by $\theta(\mathbf{a}) = a_j$ if $\mathbf{a} \in A_j$. Since the A_j are definable, θ is a definable function. Then we claim that

$$Z(h, k, \mathcal{M}, s) = \int_S |\theta(H_1(M))^{\delta_1} \cdots \theta(H_m(M))^{\delta_m}|^s \\ |\theta(K_1(M))^{\epsilon_1} \cdots \theta(K_n(M))^{\epsilon_n}| \mathrm{d}\nu.$$

This follows, since if we define

$$\mathcal{M}_{ij} = \{(g_1, \ldots, g_r) \in \mathcal{M} \mid h(g_1, \ldots, g_r) = i, k(g_1, \ldots, g_r) = j\},$$
$$S_{ij} = \{M \in \mathrm{M}_{r\times d} \mid |\theta(H_1(M))^{\delta_1} \cdots \theta(H_m(M))^{\delta_m}| = p^{-i}, \\ |\theta(K_1(M))^{\epsilon_1} \cdots \theta(K_n(M))^{\epsilon_n}| = p^{-j}\},$$

then $\mathcal{M}_{ij} = \phi(S_{ij})$ and, by part (iii) of Lemma 1.20 and part (i) of Theorem 1.8, $\mu(\mathcal{M}_{ij}) = \nu(S_{ij})$. The result then follows from part (ii) of Theorem 1.8. □

Although we have seen that the rationality follows simply by translating our group-theoretic integrals to the definable integrals of subsection 1.1, it would be interesting to see whether a suitable group-theoretic language can be devised that admits quantifier elimination for our uniform groups. Combined perhaps with some cell-decomposition theorem, we could then evaluate these

integrals within the context of the language of group theory, with the hope that some group-theoretic interpretation can be given to the rational functions. Some hope for such a cell decomposition may arise from the connections with 0-minimal sets, p-adic analytic groups and such a cell decomposition. As we shall see later, we are unable at present to get much control of the rational functions.

2. p-adic analytic groups

We defined in the Introduction the following Poincaré series associated with a group G and prime p

$$\zeta_{G,p}(s) = \sum_{n=0}^{\infty} a_{p^n}(G)p^{-ns},$$

where $a_n(G)$ denotes the number of subgroups of index n in G. We prove in this section that if G is a compact p-adic analytic group, then $\zeta_{G,p}(s)$ is a rational function in p^{-s}. We shall prove this in two stages. In subsection 2.1 we consider the special case in which G is a uniformly powerful pro-p-group. We show how to express $\zeta_{G,p}(s)$ as a definable integral in $\mathcal{L}_G$. We can then apply Theorem 1.17 to deduce the rationality of $\zeta_{G,p}(s)$. In subsection 2.2 we show how to extend the integral considered in subsection 2.1 to count subgroups in a finite extension of a uniformly powerful group and then appeal to Theorem 1.16 to deduce Theorem B. We also point out that Theorem B is the best possible for the class of pro-p-groups. The section ends with some examples calculated by Ilani. In subsection 2.3 we consider variants of our Poincaré series in which we restrict our attention to counting subgroups with various particular properties.

2.1. *Uniformly powerful pro-p-groups.* Throughout the rest of this section we fix G to be a uniformly powerful pro-p-group with $d(G) = d$. We also fix a topological generating set $\{x_1, \ldots, x_d\}$ for G. We prove the following special case of Theorem B:

THEOREM 2.1. *Let G be a uniformly powerful pro-p-group. Then $\zeta_{G,p}(s)$ is a rational function in p^{-s}.*

For each $n \geq 1$ we shall set $G_n = P_n(G)$, the n^{th} term of the lower p-series of G. Recall that the p^{th} power map $x \mapsto x^p$ induces an isomorphism

$$f_i : G_i/G_{i+1} \to G_{i+1}/G_{i+2},$$

where if $x = \mathbf{x}(\boldsymbol{\lambda}) \in G_i$, then $f_i(\mathbf{x}(\boldsymbol{\lambda}))G_{i+1} = \mathbf{x}(p\boldsymbol{\lambda})G_{i+2}$. Let $\pi : \mathbb{Z}_p \to \mathbb{F}_p$ denote the residue map. Define a map for each $n \geq 1$

$$\pi_n : G_n \to \mathbb{F}_p^d$$

by $\pi_n(\mathbf{x}(\boldsymbol{\lambda})) = (\pi(p^{-(n-1)}\lambda_1), \ldots, \pi(p^{-(n-1)}\lambda_d))$. Then π_n is a homomorphism with $\ker \pi_n = G_{n+1}$.

The philosophy behind the proof of this theorem is to express $\zeta_{G,p}(s)$ as a definable integral. The key to such an expression is the following definition:

Definition 2.2. Let H be an open subgroup in G. We define a d-tuple $(h_1, \ldots, h_d)$ of elements of H to be a *good basis* for H if

(i) $\omega(h_i) \leq \omega(h_j)$ whenever $i \leq j$, and

(ii) setting $I_n = \{j \mid \omega(h_j) = n\}$, $\{\pi_n(h_j) \mid j \in I_n\}$ extends the linearly independent set $\{\pi_n(h_j^{p^{n-\omega(h_j)}}) \mid j \in I_1 \cup \cdots \cup I_{n-1}\}$ to a basis for $\pi_n(H \cap G_n)$.

Remarks. (i) Since $f_i : G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ is an isomorphism, the set $\{\pi_n(h_j^{p^{n-\omega(h_j)}}) \mid j \in I_1 \cup \cdots \cup I_{n-1}\}$ is a linearly independent subset of $\pi_n(H \cap G_n)$.

(ii) A good basis for G is precisely a minimal topological generating set for G.

(iii) The set I_n is independent of the choice of a good basis.

Definition 2.3. If $(h_1, \ldots, h_d)$ is a good basis for the open subgroup H, then define

$$\mathrm{e}(n, j) = \max\{n - \omega(h_j), 0\}$$

for each $n \geq 1$ and $j = 1, \ldots, d$.

LEMMA 2.4. *Let H be an open subgroup with a good basis $(h_1, \ldots, h_d)$.*

(i) *If $h \in H$, then there exist $\lambda_1, \ldots, \lambda_d \in \mathbb{Z}_p$ such that*

$$h = h_1^{\lambda_1} \cdots h_d^{\lambda_d} = \mathbf{h}(\boldsymbol{\lambda}), \text{ say.}$$

(ii) *If $h = h_1^{\lambda_1} \cdots h_d^{\lambda_d}$, then $\omega(h) = \min\{\omega(h_i) + v(\lambda_i) \mid i = 1, \ldots, d\}$.*

Proof. (i) It suffices to define, for each $i = 1, \ldots, d$ and $j \geq 1$, $\lambda_i(j) \in \mathbb{Z}$ such that $\lambda_i(j) - \lambda_i(j+1) \in p^{\mathrm{e}(j,i)}\mathbb{Z}$ and

$$h \equiv h_1^{\lambda_1(j)} \cdots h_d^{\lambda_d(j)} \pmod{G_{j+1}}.$$

We define $\lambda_i(j)$ recursively. Note that, for $k \geq 1$, $\{h_1^{p^{\mathrm{e}(k,1)}}, \ldots, h_d^{p^{\mathrm{e}(k,d)}}\}$ generates $H \cap G_k$ modulo G_{k+1}. This provides our base step and the key to our recursion. Suppose that we have defined $\lambda_i(j)$ for $1 \leq j < k$. Then

$$h \equiv h_1^{\lambda_1(k-1)} \cdots h_d^{\lambda_d(k-1)} \pmod{G_k}.$$

So for some $g_k \in H \cap G_k$ it follows that

$$h \equiv h_1^{\lambda_1(k-1)} \cdots h_d^{\lambda_d(k-1)} \cdot g_k \pmod{G_{k+1}}.$$

Now there exist $\mu_1, \dots, \mu_d \in \mathbb{Z}$ such that

$$g_k \equiv h_1^{\mu_1 p^{e(k,1)}} \cdots h_d^{\mu_d p^{e(k,d)}} \pmod{G_{k+1}}.$$

But note that G_k/G_{k+1} is central in G/G_{k+1} by the definition of the lower p-series. So setting $\lambda_i(k) = \lambda_i(k-1) + p^{e(k,i)}\mu_i$, we deduce that

$$h \equiv h_1^{\lambda_1(k)} \cdots h_d^{\lambda_d(k)} \pmod{G_{k+1}}.$$

Thus setting $\lambda_i = \lim_{j\to\infty} \lambda_i(j)$ yields

$$h = h_1^{\lambda_1} \cdots h_d^{\lambda_d}.$$

(ii) Let $h = h_1^{\lambda_1} \cdots h_d^{\lambda_d}$ and define $n = \min\{\omega(h_i) + v(\lambda_i) \mid i = 1, \dots, d\}$. Then $h \in G_n$. Suppose that $h \in G_{n+1}$. Then $\pi_n(h) = 0$. Since

$$\{\pi_n(h_i^{p^{e(n,i)}}) \mid i \in I_1 \cup \cdots \cup I_n\}$$

is a basis for $\pi_n(H \cap G_n)$, this would imply that $v(p^{-e(n,i)}\lambda_i) \geq 1$ for each $i = 1, \dots, d$; i.e., $\omega(h_i) + v(\lambda_i) \geq n+1$. Consequently $h \notin G_{n+1}$; i.e., $n = \omega(h)$. □

LEMMA 2.5. *$(h_1, \dots, h_d)$ is a good basis for some open subgroup of G if and only if*

(i) *$\omega(h_i) \leq \omega(h_j)$ whenever $i \leq j$;*
(ii) *$h_i \neq 1$ for $i = 1, \dots, d$;*
(iii) *$\{h_1^{\lambda_1} \cdots h_d^{\lambda_d} \mid \lambda_i \in \mathbb{Z}_p\}$ is a subgroup of G; and*
(iv) *for all $\lambda_1, \dots, \lambda_d \in \mathbb{Z}_p$, $\omega(h) = \min\{\omega(h_i) + v(\lambda_i) \mid i = 1, \dots, d\}$.*

Proof. Lemma 2.4 establishes one half of this lemma. Conversely suppose that parts (i)-(iv) hold and let $H = \{h_1^{\lambda_1} \cdots h_d^{\lambda_d} \mid \lambda_i \in \mathbb{Z}_p\}$, a subgroup in G by part (iii). By part (iv), $H \cap G_k = \{h_1^{\lambda_1} \cdots h_d^{\lambda_d} \mid \lambda_i \in p^{e(k,i)}\mathbb{Z}_p\}$. Thus $\{\pi_k(h_i^{p^{e(k,i)}}) \mid i \in I_1 \cup \cdots \cup I_k\}$ generates $\pi_k(H \cap G_k)$. (Note that $\pi_k(h_i) = 0$ if $i \in I_j$ for $j > k$.) The linear independence of $\{\pi_k(h_i^{p^{e(k,i)}}) \mid i \in I_1 \cup \cdots \cup I_k\}$ is equivalent to the nonexistence of $\lambda_i \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$ with the property that $\omega(h_1^{\lambda_1 p^{e(k,1)}} \cdots h_m^{\lambda_m p^{e(k,m)}}) > k$, where $m = \operatorname{card}(I_1 \cup \cdots \cup I_k)$. Since $\omega(h^\lambda) = \omega(h) + v(\lambda)$, the linear independence of this set follows from part (iv). Finally we must prove that H is open. By part (ii) there exists $n \in \mathbb{N}$ (i.e., $n = \omega(h_d)$) such that $\pi_n(H \cap G_n)$ is a subspace of dimension d. Thus $\pi_n(H \cap G_n) = \pi_n(G_n)$; i.e., $H \geq G_n$. □

LEMMA 2.6. *Let $(h_1, \dots, h_d)$ be a good basis for the open subgroup H in G. Let $s_n = \operatorname{card} I_n$ and suppose that $h_1', \dots, h_d'$ are elements in H with $h_i' = h_1^{a_{i1}} \cdots h_d^{a_{id}}$, where $a_{ij} \in \mathbb{Z}_p$. Then $(h_1', \dots, h_d')$ is a good basis for H if and only if $a_{ij} \in p^{e(\omega(h_i),j)}\mathbb{Z}_p$ and, whenever $s_n \neq 0$, then $(a_{ij})_{i,j\in I_n} \in \mathrm{GL}_{s_n}(\mathbb{Z}_p)$.*

Proof. The d-tuple $(h_1', \dots, h_d')$ is a good basis for H if and only if
(i) for each $i = 1, \dots, d$, $\omega(h_i') = \omega(h_i)$, and
(ii) for each n, $\{\pi_n(h_i') \mid i \in I_n\}$ is a basis for $\pi_n(H \cap G_n)$ modulo $\pi_n(H^p \cap G_n)$.
Now $\omega(h_i') \geq \omega(h_i)$ if and only if $a_{ij} \in p^{e(\omega(h_i),j)}\mathbb{Z}_p$. Condition (ii) holds if and only if $(\pi(a_{ij}))_{i,j\in I_n} \in \mathrm{GL}_{s_n}(\mathbb{F}_p)$; i.e., $(a_{ij})_{i,j\in I_n} \in \mathrm{GL}_{s_n}(\mathbb{Z}_p)$. This also ensures that $\omega(h_i') = \omega(h_i)$ and thus proves the lemma. □

We associate with each subgroup H of finite index in G the subset $M(H)$ of $G^{(d)}$ consisting of all d-tuples $(h_1, \dots, h_d)$, which are good bases for H. Let $(h_1, \dots, h_d)$ be a good basis for H and define $q_i = p^{\omega(h_i)-1}$, which is independent of our choice of a good basis.

LEMMA 2.7. *Let H be a subgroup of finite index in G. Then $M(H)$ is an open subset of $G^{(d)}$ and*

$$\mu(M(H)) = (1 - p^{-1})^d \prod_{i=1}^{d} q_i^{-i} \cdot q_{i+1}^{-1} \cdots q_d^{-1}.$$

Proof. The subgroup H is open in G so that $G_m \leq H$ for some m. To prove that $M(H)$ is open it suffices to show that for all $(h_1, \dots, h_d) \in M(H)$

$$(h_1', \dots, h_d') \in M(H),$$

where $h_i' = h_i g_i$ and $g_i \in G_{m+1}$. Since $\pi_n(h_i) = \pi_n(h_i')$ for all $n \leq m$, this follows from the definition of a good basis for H. Thus $M(H)$ is open and therefore measurable.

We fix a good basis $(h_1, \dots, h_d)$ for H. Since the p^{th} power map induces the isomorphism $f_i : P_i(G)/P_{i+1}(G) \to P_{i+1}(G)/P_{i+2}(G)$ for each $i \geq 1$, there exists a good basis $(y_1, \dots, y_d)$ for G with the property that $y_i^{q_i} = h_i$, where $q_i = p^{\omega(h_i)-1}$. Define

$$\phi : \mathrm{M}_d(\mathbb{Z}_p) \to G^{(d)}$$

by $\phi(M) = (\mathbf{y}(\mathbf{m}_1), \dots, \mathbf{y}(\mathbf{m}_d))$, where $\mathbf{m}_i$ denotes the i^{th} row of the matrix $M \in \mathrm{M}_d(\mathbb{Z}_p)$. Let

$$A = \{(a_{ij}) \in \mathrm{M}_d(\mathbb{Z}_p) \mid a_{ij} \in q_j p^{e(\omega(h_i),j)}\mathbb{Z}_p \text{ and, whenever } s_n \neq 0, \text{ then } (q_j^{-1}a_{ij})_{i,j\in I_n} \in \mathrm{GL}_{s_n}(\mathbb{Z}_p)\}.$$

Then, by Lemma 2.6, $\phi(A) = M(H)$, where ϕ was defined in Lemma 1.20. By part (iii) of Lemma 1.20, $\mu(M(H)) = \nu(A)$. For each $s_k \neq 0$ we calculate the measure of the block

$$A_k = \{(a_{ij}) \in \mathrm{M}_{s_k \times d}(\mathbb{Z}_p) \mid i \in I_k \text{ and } \mathbf{a}_i \text{ is the } i^{\text{th}} \text{ row of some } M \in A\}.$$

By the definition of $\mathrm{e}(\omega(h_i), j)$ we have

$$q_j p^{\mathrm{e}(\omega(h_i),j)} = \begin{cases} q_j & \text{if } i \leq j, \\ q_i & \text{if } i > j. \end{cases}$$

The measure of $\mathrm{GL}_{s_k}(\mathbb{Z}_p)$ is equal to $(1-p^{-1})^{s_k}$. Therefore

$$\nu(A_k) = (1-p^{-1})^{s_k} \prod_{i \in I_k} q_i^{-i} \cdot q_{i+1}^{-1} \cdots q_d^{-1}.$$

Since $I_1 \cup \cdots \cup I_m = \{1, \ldots, d\}$, $A = A_1 \times \cdots \times A_m$ and $\nu(X \times Y) = \nu(X) \cdot \nu(Y)$, it follows that

$$\begin{aligned} \nu(A) &= (1-p^{-1})^{s_1+\cdots+s_m} \prod_{i \in I_1 \cup \cdots \cup I_m} q_i^{-i} \cdot q_{i+1}^{-1} \cdots q_d^{-1} \\ &= (1-p^{-1})^d \prod_{i=1}^{d} q_i^{-i} \cdot q_{i+1}^{-1} \cdots q_d^{-1}, \end{aligned}$$

proving the lemma. □

Using Lemma 2.7, we can express our Poincaré series in the form of a group-theoretic integral. We define for each $i = 1, \ldots, d$ the function $f_i : G^{(d)} \to G$ by $f_i(g_1, \ldots, g_d) = g_i$. Let H be a subgroup of finite index in G. Recall the definition of q_i given above Lemma 2.7. For all $(h_1, \ldots, h_d) \in M(H)$, $p^{\omega(f_i(h_1,\ldots,h_d))-1} = q_i$. Note that

$$\begin{aligned} |G : H| &= \prod_{i \geq 1} |G_i H : G_{i+1} H| = \prod_{i \geq 1} |G_i : G_i \cap G_{i+1} H| \\ &= p^{\omega(h_1)-1} \cdots p^{\omega(h_d)-1} = q_1 \cdots q_d. \end{aligned}$$

Define $h : G^{(d)} \to \mathbb{N}$ and $k : G^{(d)} \to \mathbb{N}$ by

$$\begin{aligned} h(g_1, \ldots, g_d) &= \omega\big(f_1(g_1, \ldots, g_d)\big) + \cdots + \omega\big(f_d(g_1, \ldots, g_d)\big), \\ k(g_1, \ldots, g_d) &= \sum_{i=1}^{d} (2i-1)\omega\big(f_i(g_1, \ldots, g_d)\big). \end{aligned}$$

Then

$$|G : H|^{-s} = (1-p^{-1})^{-d} \prod_{i=1}^{d} p^{s-2i+1} \int_{M(H)} p^{-sh(g_1,\ldots,g_d)+k(g_1,\ldots,g_d)} \mathrm{d}\mu.$$

Defining $\mathcal{M} = \bigcup_{H \leq_p G} M(H)$ leads to

$$\zeta_{G,p}(s) = (1-p^{-1})^{-d} \prod_{i=1}^{d} p^{s-2i+1} \int_{\mathcal{M}} p^{-sh(g_1,\ldots,g_d)+k(g_1,\ldots,g_d)} \mathrm{d}\mu. \tag{2.1}$$

LEMMA 2.8. (a) *The functions f_i are definable for each $i = 1, \dots, d$.*
(b) *$\mathcal{M}$ is a definable subset of $G^{(d)}$.*

Proof. Part (a) follows immediately from the definition of f_i. For part (b) it follows from Lemma 2.5 that $(h_1, \dots, h_d) \in \mathcal{M}$ if and only if

(i) $\omega(h_i) \leq \omega(h_j)$ for $i \leq j$;
(ii) $h_i \neq 1$ for each $i = 1, \dots, d$;
(iii) for all $\boldsymbol{\lambda}, \boldsymbol{\mu} \in \mathbb{Z}_p^d$ there exists $\boldsymbol{\nu} \in \mathbb{Z}_p^d$ such that

$$h_1^{\nu_1} \cdots h_d^{\nu_d} = h_1^{\lambda_1} \cdots h_d^{\lambda_d} (h_1^{\mu_1} \cdots h_d^{\mu_d})^{-1};$$

(iv) for all $\boldsymbol{\lambda} \in \mathbb{Z}_p^d$

$$\omega(h_1^{\lambda_1} \cdots h_d^{\lambda_d}) = \min\{\omega(h_i^{\lambda_i}) \mid i = 1, \dots, d\}.$$

Since $h_i = f_i(h_1, \dots, h_d)$ is a definable function, the conjunction of statements (i)-(iv) is a formula in $\mathcal{L}_G$ defining the subset $\mathcal{M}$. □

Proof of Theorem 2.1. In equation (2.1) we expressed $\zeta_{G,p}(s)$ as a group-theoretic integral. By Lemma 2.8 this integral is definable in $\mathcal{L}_G$. Thus we are in a position to apply Theorem 1.17 to deduce that $\zeta_{G,p}(s)$ is a rational function in p^{-s}. □

2.2. *Compact p-adic analytic groups.* Let G be a compact p-adic analytic group. By Theorem 1.16 there exists a uniformly powerful normal subgroup G_1 of finite index in G. Let K be a subgroup of G with the property that $G_1 \leq K$. Define

$$\zeta_{G,p}^K(s) = \sum_{H \in \mathcal{H}(K)} |K : H|^{-s},$$

where $\mathcal{H}(K) = \{H \leq K \mid G_1 H = K\}$. In this part we show how to extend the integral constructed in subsection 2.1 to prove the following:

THEOREM 2.9. *$\zeta_{G,p}^K(s)$ is a rational function in p^{-s}.*

Theorem 2.9 suffices to prove Theorems B and C, since

$$\zeta_{G,p}(s) = \sum_{G_1 \leq K \leq_p G} |G : K|^{-s} \zeta_{G,p}^K(s),$$

$$\zeta_G(s) = \sum_{G_1 \leq K \leq G} |G : K|^{-s} \zeta_{G,p}^K(s).$$

Throughout the rest of this section we fix a right transversal $(y_1, \dots, y_n)$ for G_1 in K with $y_1 = 1$ and a good basis $(x_1, \dots, x_d)$ for G_1. The following concept is the key to expressing $\zeta_{G,p}^K(s)$ as a definable integral.

Definition 2.10. Let $H \in \mathcal{H}(K)$. We call $(t_1, \ldots, t_n)$ a *transversal basis* for H if

(i) $t_i \in G_1$ for each $i = 1, \ldots, n$, and

(ii) $(t_1 y_1, \ldots, t_n y_n)$ is a right transversal for $H_1 = H \cap G_1$ in H.

We call $(h_1, \ldots, h_d, t_1, \ldots, t_n)$ a *basis* for H if $(h_1, \ldots, h_d)$ is a good basis for $H_1 = H \cap G_1$ and $(t_1, \ldots, t_n)$ is a transversal basis for H.

With each subgroup H of finite index in G we associate the subset $T(H)$ of $G_1^{(n)}$ consisting of transversal bases for H.

LEMMA 2.11. *Let $H \in \mathcal{H}(K)$. Then $T(H)$ is an open subset of $G_1^{(n)}$ and*

$$\mu(T(H)) = |G_1 : H_1|^{-n}.$$

Proof. If we fix a transversal basis $(t_1, \ldots, t_n)$ for H, then

$$T(H) = H_1 t_1 \times \cdots \times H_1 t_n. \tag{2.2}$$

The coset $H_1 t_i$ is an open subset of G_1 with Haar measure $|G_1 : H_1|^{-1}$. The lemma now follows from equation (2.2). □

Let $N(H) = M(H_1) \times T(H)$, i.e., the set of bases for H. We define for each $i = 1, \ldots, d$ the function $f_i : G^{(d+n)} \to G$ by $f_i(g_1, \ldots, g_{d+n}) = g_i$. Define $h : G^{(d+n)} \to \mathbb{N}$ and $k : G^{(d+n)} \to \mathbb{N}$ by

$$h(g_1, \ldots, g_{d+n}) = \omega\big(f_1(g_1, \ldots, g_{d+n})\big) + \cdots + \omega\big(f_d(g_1, \ldots, g_{d+n})\big), \tag{2.3}$$

$$k(g_1, \ldots, g_{d+n}) = \sum_{i=1}^{d} (2i + n - 1)\omega\big(f_i(g_1, \ldots, g_{d+n})\big). \tag{2.4}$$

Then by Lemma 2.11

$$\begin{aligned} |K : H|^{-s} &= |G_1 : H_1|^{-s} \\ &= (1 - p^{-1})^{-d} \prod_{i=1}^{d} p^{s-2i+1-n} \int_{N(H)} p^{-sh(g_1,\ldots,g_{d+n}) + k(g_1,\ldots,g_{d+n})} \mathrm{d}\mu. \end{aligned}$$

Defining $\mathcal{N}(K) = \bigcup_{H \in \mathcal{H}(K)} N(H)$ leads to

$$\begin{aligned} \zeta_{G,p}^{K}(s) &= (1 - p^{-1})^{-d} \prod_{i=1}^{d} p^{s-2i+1-n} \int_{\mathcal{N}(K)} p^{-sh(g_1,\ldots,g_{d+n}) + k(g_1,\ldots,g_{d+n})} \mathrm{d}\mu \\ &= c \int_{\mathcal{N}(K)} F(g_1, \ldots, g_{d+n}) \mathrm{d}\mu, \text{ say.} \end{aligned} \tag{2.5}$$

LEMMA 2.12. *$\mathcal{N}(K)$ is a definable subset of $G_1^{(d+n)}$.*

Proof. The $(d+n)$-tuple $(h_1,\dots,h_d,t_1,\dots,t_n) \in \mathcal{N}(K)$ if and only if $(h_1,\dots,h_d)$ is a good basis for some subgroup H_1 of G_1 and the set $X = H_1t_1y_1 \cup \cdots \cup H_1t_ny_n$ is a subgroup of G. The set X is a subgroup provided that

$$ht_iy_i(h't_jy_j)^{-1} \in X \tag{2.6}$$

for all $h, h' \in H_1$ and $i,j = 1,\dots,n$. Define $a_{ij}, b_i \in G_1$ along with

$$\gamma : \{1,\dots,n\}^2 \to \{1,\dots,n\} \quad \text{and} \quad \delta : \{1,\dots,n\} \to \{1,\dots,n\}$$

by

$$y_iy_j = a_{ij}y_{\gamma(i,j)},$$
$$y_i^{-1} = b_iy_{\delta(i)}.$$

Since G_1 is normal in G, it is a straightforward exercise to check that (2.6) is equivalent to the following condition

$$ht_iy_i\big(b_jy_{\delta(j)}(t_j^{-1}h'^{-1})y_{\delta(j)}^{-1}\big)y_i^{-1}a_{i\delta(j)} = h''t_{\gamma(i,\delta(j))}$$

for some $h'' \in H_1$. So, by Lemma 2.8 and the above, the set $\mathcal{N}(K)$ is definable by a statement in $\mathcal{L}_G$, where we include automorphisms in $\mathcal{L}_G$ for conjugation by each transversal element y_i. □

Proof of Theorem 2.9. In equation (2.5) we expressed $\zeta_{G,p}^K(s)$ as a group-theoretic integral. By Lemma 2.12 this integral is definable in $\mathcal{L}_G$. Thus we are in a position to apply Theorem 1.17 to deduce that $\zeta_{G,p}^K(s)$ is a rational function in p^{-s}. □

For the class of pro-p-groups, Theorem B is the best possible in the following sense:

THEOREM 2.13. *Let G be a pro-p-group. Suppose that $\zeta_{G,p}(s)$ is a rational function in p^{-s}. Then G is a p-adic analytic group.*

Proof. By [LuM2], Theorem 3.1, or [DxduSMS], Theorem 3.19, it suffices to prove that $a_{p^n} = a_{p^n}(G)$ grows at most polynomially with p^n. As we pointed out in the Introduction, $\zeta_{G,p}(s)$ being rational is equivalent to the coefficients a_{p^n} satisfying a recurrence relation

$$a_{p^n} + c_1a_{p^{n-1}} + \cdots + c_ka_{p^{n-k}} = 0,$$

where $n \geq l$ and $c_1,\dots,c_k$ are independent of n. It follows that

$$|a_{p^n}| \leq KC^n,$$

where K is independent of n and $C = |c_1| + \cdots + |c_k|$. Hence

$$|a_{p^n}| \leq K(p^n)^{\log_p C};$$

i.e., a_{p^n} grows at most polynomially. □

We conclude this section with some examples calculated by Ilani [Il].

Examples 2.14. Let $G = \mathrm{SL}_2(\mathbb{Z}_p)$ and denote by $G(i)$ the i^{th} principal congruence subgroup

$$1 \to G(i) \to G \to \mathrm{SL}_2(\mathbb{Z}_p/p^i\mathbb{Z}_p) \to 1.$$

We use the shorthand notation introduced in [GSSm] for the following rational functions in p^{-s}:

$$X_b^a = p^{b-as}, \quad P_b^a = (1 - X_b^a)^{-1}, \quad Z_n = P_0^1 P_1^1 \dots P_{n-1}^1.$$

Then

$$\begin{aligned}\zeta_{G(i),p}(s) = \zeta_{G(i)}(s) = Z_3 - X_{2i+1}^{i+1} P_1^0 \Big(& X_4^0 P_2^0 P_2^1 + (p+1) P_1^1 P_2^2 \\ & - \big(X_1^1(p^3 - p - 1) - 1\big) P_2^0 P_2^2 \\ & - (1 + X_1^0) P_1^0 P_1^2 \Big).\end{aligned}$$

2.3. *Variations.* In this part we study some variants of the Poincaré series considered in the previous sections. Although we only consider functions, counting subgroups of p-power index, clearly we can prove similar results to Theorem C for the corresponding global Dirichlet series.

2.3.1. *Normal subgroups.* Define

$$\mathcal{H}^{\triangleleft} = \{H \leq_p G \mid \text{ is a } \textit{normal} \text{ subgroup in } G\}.$$

We consider the following Poincaré series associated with this set of subgroups:

$$\zeta_{G,p}^{\triangleleft}(s) = \sum_{H \in \mathcal{H}^{\triangleleft}} |G : H|^{-s}.$$

THEOREM 2.15. *Let G be a compact p-adic analytic group. Then $\zeta_{G,p}^{\triangleleft}(s)$ is a rational function in p^{-s}.*

Proof. Let G_1 be a uniformly powerful subgroup of G and K be a normal subgroup of G with the property that $G_1 \leq K$. Fix a good basis $(x_1, \dots, x_d)$ for G_1 and a right transversal $(y_1, \dots, y_m)$ for G_1 in G with the property that $(y_1, \dots, y_n)$ is a right transversal for G_1 in K. For each $i = 1, \dots, n$, $j = 1, \dots, d$ and $k = 1, \dots, m$ we define a_{ij} and $b_{ik} \in G_1$ such that

$$\begin{aligned} x_j^{-1} y_i x_j &= a_{ij} y_{\phi(i,j)}, \\ y_k^{-1} y_i y_k &= b_{ik} y_{\psi(i,k)}, \end{aligned}$$

where $\phi(i,j)$ and $\psi(i,k) \in \{1,\dots,n\}$. Define

$$\mathcal{H}^{\triangleleft}(K) = \{H \in \mathcal{H}^{\triangleleft} \mid G_1 H = K\}$$

and

$$\zeta_{G,p}^{K,\triangleleft}(s) = \sum_{H \in \mathcal{H}^{\triangleleft}(K)} |K:H|^{-s}.$$

As in the proof of Theorem B, it suffices to prove the rationality of $\zeta_{G,p}^{K,\triangleleft}(s)$. Let

$$\mathcal{N}(K)^{\triangleleft} = \bigcup_{H \in \mathcal{H}^{\triangleleft}(K)} N(H).$$

Then

$$\zeta_{G,p}^{K,\triangleleft}(s) = c \int_{\mathcal{N}(K)^{\triangleleft}} F(g_1,\dots,g_{d+n}) \mathrm{d}\mu,$$

where c and $F(g_1,\dots,g_{d+n})$ are defined as in equation (2.5). Thus Theorem 2.15 reduces to proving that $\mathcal{N}(K)^{\triangleleft}$ is definable. Let $(h_1,\dots,h_d,t_1,\dots,t_n) \in \mathcal{N}(K)$. There exists $H \in \mathcal{H}(K)$ such that $(h_1,\dots,h_d)$ is a good basis for $H_1 = H \cap G_1$ and $(t_1,\dots,t_n)$ is a transversal basis for H. Now H is normal in G if and only if, for each $i,j = 1,\dots,d$ and $k = 1,\dots,m$ and $l = 1,\dots,n$, we have

(a) $x_j^{-1} h_i x_j \in H_1$;

(b) $y_k^{-1} h_i y_k \in H_1$;

(c) there exists $h \in H_1$ such that $x_j^{-1} t_l x_j a_{lj} = h t_{\phi(l,j)}$; and

(d) there exists $h \in H_1$ such that $y_k^{-1} t_l y_k b_{lk} = h t_{\psi(l,k)}$.

Each of the conditions (a)-(d) reduces to a definable formula in $\mathcal{L}_G$. The conjunction of these formulae with the formula in $\mathcal{L}_G$ defining the subset $\mathcal{N}(K)$ defines the set $\mathcal{N}(K)^{\triangleleft}$. Since $\mathcal{N}(K)^{\triangleleft}$ is definable, $\zeta_{G,p}^{K,\triangleleft}(s)$ is rational in p^{-s}. □

2.3.2. *r-Generated subgroups.* For each $r \in \mathbb{N}$ define

$$\mathcal{H}(r) = \{H \leq_p G \mid d(H) = r\}.$$

Note that if G is a compact p-adic analytic group, then G has finite rank. This implies that $\mathcal{H}(r)$ is empty for sufficiently large r. We define

$$\zeta_{G,p}^{r}(s) = \sum_{H \in \mathcal{H}(r)} |G:H|^{-s}.$$

Then $\zeta_{G,p}(s) = \sum_{r \in \mathbb{N}} \zeta_{G,p}^{r}(s)$. In [M], A. Mann has observed that if G is a p-adic analytic pro-p-group, these Poincaré series satisfy a simple functional equation

$$\sum_{l=1}^{d} \big(\zeta_p(s) \cdots \zeta_p(s-l+1)\big)^{-1} \zeta_{G,p}^{l}(s) = 1,$$

where $\zeta_p(s) = (1-p^{-s})^{-1}$ is the local Riemann zeta function and d is the rank of G. We shall prove the following theorem:

THEOREM 2.16. *Let G be a p-adic analytic pro-p-group. Then $\zeta^r_{G,p}(s)$ is rational in p^{-s} for each $r \in \mathbb{N}$.*

First we shall need some preparatory lemmas. Recall that the Frattini subgroup of a profinite group is defined by

$$\Phi(G) = \bigcap \{M \mid M \text{ is a maximal, proper, open subgroup of } G\}.$$

It has the property that $d(G) = d(G/\Phi(G))$. If G is a pro-p-group, then $\Phi(G) = P_2(G)$ and $G/\Phi(G)$ is an elementary abelian group. Consequently

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

For the rest of this section we fix the following notation: Let G_1 be a normal uniform pro-p-group in the p-adic analytic pro-p-group G and let K be a subgroup of G with $G_1 \leq K \leq G$. Let $\{y_1, \ldots, y_n\}$ be a transversal for the right cosets of G_1 in K such that $\{y_1, \ldots, y_s\}$ $(s \leq n)$ is a transversal for G_1 in $G_1\Phi(K)$.

LEMMA 2.17. *Let H be a subgroup of G with $K = G_1H$. Then*

$$\Phi(H) = \Phi(K)G_1 \cap \bigcap \{M \mid M \leq H, M_1 = M \cap G_1 \text{ is maximal in } H_1,\ MH_1 = H\}.$$

Proof. Let M be a maximal subgroup of H. Then either
(i) $MG_1 = L$, a maximal subgroup of K and $M \cap G_1 = H_1$, or
(ii) $MH_1 = H$ and $M \cap G_1 = M_1$, a maximal subgroup of H_1.
If $G_1 \leq L \leq K$ and L is maximal in K, then $M = L \cap H$ is a maximal subgroup of type (i) in H. Thus the intersection of maximal subgroups of type (i) is $\Phi(K)G_1 \cap H$. Intersecting these with the maximal subgroups of type (ii), we have the desired result. □

LEMMA 2.18. *There exists a formula $\phi(\mathbf{X}, \mathbf{Y})$ in $\mathcal{L}_G$ such that $\phi(\mathbf{x}, \mathbf{y})$ is true if and only if $\mathbf{x}$ is a good basis for a subgroup H of G_1 and $\mathbf{y}$ is a good basis for a maximal subgroup M of H.*

Proof. Let $\theta(\mathbf{X})$ be the formula ensuring that $\mathbf{x}$ is a good basis for some subgroup. If $\mathbf{x}$ and $\mathbf{y}$ are good bases for the subgroups H and J, then $J \subseteq H$ provided that for each $i = 1, \ldots, d$ there exists $(\lambda_1, \ldots, \lambda_d) \in \mathbb{Z}_p^d$ such that

$$y_i = x_1^{\lambda_1} \cdots x_d^{\lambda_d}.$$

Let $\sigma(\mathbf{X}, \mathbf{Y})$ be this statement. Define the formula $\tau(\mathbf{X}, \mathbf{Y})$ by

$$(\text{for all } \mathbf{Z})\big(\theta(\mathbf{Z}) \wedge \sigma(\mathbf{Z}, \mathbf{Y}) \wedge \sigma(\mathbf{X}, \mathbf{Z}) \to \sigma(\mathbf{Z}, \mathbf{X}) \vee \sigma(\mathbf{Y}, \mathbf{Z})\big).$$

Then

$$\phi(\mathbf{X}, \mathbf{Y}) = \theta(\mathbf{X}) \wedge \theta(\mathbf{Y}) \wedge \sigma(\mathbf{X}, \mathbf{Y}) \wedge \tau(\mathbf{X}, \mathbf{Y}). \qquad \square$$

LEMMA 2.19. *For each $i = 1, \dots, n$ there exists a formula $\Phi_i(\mathbf{X}, \mathbf{Y}, Z)$ with the property that $\Phi_i(h_1, \dots, h_d, t_1, \dots, t_s, z)$ is true if and only if*

(i) *$(h_1, \dots, h_d, t_1, \dots, t_s)$ is a basis for some subgroup $H \in \mathcal{H}(K)$; and*

(ii) *$zy_i \in \Phi(H)$.*

Proof. If $i \notin \{1, \dots, s\}$, then take $\Phi_i(\mathbf{X}, \mathbf{Y}, Z)$ to be any contradiction. Suppose that $i \in \{1, \dots, s\}$. Let $\theta(\mathbf{X}, \mathbf{Y})$ be the formula provided by Lemma 2.12 with the property that $\theta(h_1, \dots, h_d, t_1, \dots, t_s)$ is true if and only if $(h_1, \dots, h_d, t_1, \dots, t_s) \in \mathcal{N}(K)$. We first require a formula $\chi(\mathbf{X}, \mathbf{Y}, \mathbf{U}, \mathbf{V})$ with the property that $\chi(\mathbf{x}, \mathbf{y}, \mathbf{u}, \mathbf{v})$ is true if and only if $(\mathbf{x}, \mathbf{y})$ is a basis for a subgroup H and $(\mathbf{u}, \mathbf{v})$ is a basis for a subgroup M of H with the property that $M_1 = M \cap G_1$ is maximal in H_1 and $MH_1 = H$. Let $\alpha(\mathbf{X}, \mathbf{Y}, \mathbf{V})$ be the formula in $\mathcal{L}_G$ defining when $H_1 y_i = H_1 v_i$ for $i = 1, \dots, n$. Then χ is a conjunction of the following formulae:

(i) $\theta(\mathbf{X}, \mathbf{Y})$;

(ii) $\theta(\mathbf{U}, \mathbf{V})$;

(iii) $\phi(\mathbf{X}, \mathbf{U})$; and

(iv) $\alpha(\mathbf{X}, \mathbf{Y}, \mathbf{V})$.

Let $\beta(\mathbf{X}, A)$ be the statement expressing the fact that there exists $(\lambda_1, \dots, \lambda_d) \in \mathbb{Z}_p^d$ such that

$$a = x_1^{\lambda_1} \cdots x_d^{\lambda_d}.$$

So the formula $\Phi_i(\mathbf{X}, \mathbf{Y}, Z)$ we want is

$$(\text{for all } (\mathbf{U}, \mathbf{V}))\left(\chi(\mathbf{X}, \mathbf{Y}, \mathbf{U}, \mathbf{V}) \to \beta\big(\mathbf{U}, (Z \cdot V_i^{-1})\big)\right). \qquad \square$$

LEMMA 2.20. *There exists a formula $\Omega_K(\mathbf{X}, \mathbf{Y})$ with the property that $\Omega_K(h_1, \dots, h_d, t_1, \dots, t_s)$ is true if and only if*

(i) *$(h_1, \dots, h_d, t_1, \dots, t_s)$ is a basis for some subgroup $H \in \mathcal{H}(K)$; and*

(ii) *$d(H) = r$.*

Proof. Let $y_1, \dots, y_n$ be a transversal for G_1 in K. Let $\mathbf{i} = (i_1, \dots, i_r) \in \{1, \dots, n\}^r$ and $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_r) \in \{0, \dots, p-1\}^r$. Then there exist $\epsilon(\mathbf{i}, \boldsymbol{\alpha}) \in$

$\{1,\dots,n\}$ and a definable function $F_{\mathbf{i},\boldsymbol{\alpha}}(X_1,\dots,X_r)$ in $\mathcal{L}_G$ such that, for all $g_1,\dots,g_r \in G_1$,

$$(g_1 y_{i_1})^{\alpha_1}\cdots(g_r y_{i_r})^{\alpha_r} = F_{\mathbf{i},\boldsymbol{\alpha}}(g_1,\dots,g_r)\,y_{\epsilon(\mathbf{i},\boldsymbol{\alpha})}.$$

For $i,j \in \{1,\dots,n\}$, define $\kappa(i,j) \in \{1,\dots,n\}$ and c_{ij} by $y_i(y_j)^{-1} = c_{ij}y_{\kappa(i,j)}$. Now $(h_1,\dots,h_d,t_1,\dots,t_n)$ satisfies conditions (i) and (ii) provided that

$$\begin{aligned}&(\text{there exist } \boldsymbol{\lambda}_1,\dots,\boldsymbol{\lambda}_r \in \mathbb{Z}_p^d)\\ &\Bigg(\bigvee_{\mathbf{i}\in\{1,\dots,n\}^r}\Bigg(\text{for all } \boldsymbol{\mu}\in\mathbb{Z}_p^d \bigwedge_{j\in\{1,\dots,n\}}\Bigg(\bigvee_{\boldsymbol{\alpha}\in\{0,\dots,p-1\}^r}\\ &\Phi_{\kappa(\epsilon(\mathbf{i},\boldsymbol{\alpha}),j)}\big(\mathbf{h},\mathbf{t},y_j^{-1}\big(\mathbf{h}(\boldsymbol{\mu})t_j\big)^{-1}F_{\mathbf{i},\boldsymbol{\alpha}}\big(\mathbf{h}(\boldsymbol{\lambda}_1),\dots,\mathbf{h}(\boldsymbol{\lambda}_r)\big)y_j c_{\epsilon(\mathbf{i},\boldsymbol{\alpha})j}\big)\Bigg)\Bigg)\Bigg).\end{aligned}$$

This is a definable formula in $\mathcal{L}_G$. □

Proof of Theorem 2.16. Again we only have to prove for each subgroup $K \geq G_1$ that

$$\zeta_{G,p}^{K,r}(s) = \sum_{H\in\mathcal{H}(K,r)} |K:H|^{-s}$$

is rational in p^{-s}, where $\mathcal{H}(K,r) = \{H \in \mathcal{H}(r) \mid G_1H = K\}$. Let

$$\mathcal{N}(K)^r = \bigcup_{H\in\mathcal{H}(K,r)} N(H).$$

Then

$$\zeta_{G,p}^{K,r}(s) = c\int_{\mathcal{N}(K)^r} F(g_1,\dots,g_{d+n})\mathrm{d}\mu,$$

where c and $F(g_1,\dots,g_{d+n})$ are defined as in equation (2.5). By Lemma 2.20, $\mathcal{N}(K)^r$ is a definable subset. So $\zeta_{G,p}^{K,r}(s)$ is a rational function in p^{-s}. □

2.3.3. *Conjugacy classes.* Define $C(G)$ to be a set of representatives for the conjugacy classes of subgroups of finite index in G. Define

$$a_n^{\mathrm{c}}(G) = \mathrm{card}\{H \in C(G) \mid |G:H| = n\}.$$

In this subsection we consider the following Poincaré series:

$$\zeta_{G,p}^{\mathrm{c}}(s) = \sum_{n\in\mathbb{N}} a_{p^n}^{\mathrm{c}}(G)p^{-ns}.$$

THEOREM 2.21. *If G is a compact p-adic analytic group, then $\zeta_{G,p}^{\mathrm{c}}(s)$ is a rational function in p^{-s}.*

Proof. To prove this theorem we rewrite our Poincaré series using the fact that the number of subgroups in the conjugacy class of H is $|G:\mathrm{N}_G(H)|$.

Thus

$$\begin{aligned}\zeta^{\mathrm{c}}_{G,p}(s) &= \sum_{H\leq_p G} |G:H|^{-s}|G:\mathrm{N}_G(H)|^{-1}\\ &= \sum_{G_1\leq K\lhd_p L\leq_p G} |G:K|^{-s}|G:L|^{-1}\sum_{H\in\mathcal{H}(K,L)} |K:H|^{-s}|L:\mathrm{N}_G(H)|^{-1}\\ &= \sum_{G_1\leq K\lhd_p L\leq_p G} |G:K|^{-s}|G:L|^{-1}\zeta^{\mathrm{c}(K,L)}_{G,p}(s),\end{aligned}$$

where $\mathcal{H}(K,L)=\{H \mid HG_1=K \text{ and } \mathrm{N}_G(H)G_1=L\}$. Now

$$\zeta^{\mathrm{c}(K,L)}_{G,p}(s) = \sum_{H\in\mathcal{H}(K,L)}\Big(\int_{N(H)} F_1(g_1,\dots,g_{d+n})\mathrm{d}\mu \int_{N(\mathrm{N}_G(H))} F_2(g_1,\dots,g_{d+n})\mathrm{d}\mu\Big),$$

where

$$\begin{aligned}F_1(g_1,\dots,g_{d+n}) &= cp^{-sh(g_1,\dots,g_{d+n})+k(g_1,\dots,g_{d+n})},\\ F_2(g_1,\dots,g_{d+n}) &= cp^{-h(g_1,\dots,g_{d+n})+k(g_1,\dots,g_{d+n})},\end{aligned}$$

and h and k are defined as in equations (2.3) and (2.4) and c is defined as in (2.5). So we have

$$\zeta^{\mathrm{c}(K,L)}_{G,p}(s) = \int_X F_1(g_1,\dots,g_{d+n})F_2(g_1,\dots,g_{d+n})\mathrm{d}\mu,$$

where $X=\bigcup_{H\in\mathcal{H}(K,L)} N(H)\times N(\mathrm{N}_G(H))$. The rationality of $\zeta^{\mathrm{c}}_{G,p}(s)$ then reduces to the question of whether X is definable.

Fix a good basis $(x_1,\dots,x_d)$ for G_1 and a right transversal $(y_1,\dots,y_n)$ for G_1 in G with the property that $(y_1,\dots,y_s)$ (resp. $(y_1,\dots,y_l)$, $(y_1,\dots,y_m)$) is a right transversal for K (resp. L, $\mathrm{N}_G(H)$) in G. We define $a_{ij}, b_{ik}, \phi(i,j)$ and $\psi(i,k)$ as in Theorem 2.15.

Now $((h_1,\dots,h_d,t_1,\dots,t_s),(k_1,\dots,k_d,w_1,\dots,w_l))\in X$ if and only if

(i) $(h_1,\dots,h_d,t_1,\dots,t_s)$ and $(k_1,\dots,k_d,w_1,\dots,w_l)$ are bases for some subgroups H and M, respectively; and if $H_1=H\cap G_1$, then

(ii) $k_j^{-1}h_ik_j\in H_1$ $(i,j=1,\dots,d)$;

(iii) $y_j^{-1}w_j^{-1}h_iw_jy_j\in H_1$ $(i=1,\dots,d \text{ and } j=1,\dots,l)$;

(iv) there exists $h\in H_1$ such that

$$(k_j^{-1}t_ik_j)k_j^{-1}(y_ik_jy_i^{-1}) = ht_i$$

$(i=1,\dots,s \text{ and } j=1,\dots,d)$;

(v) there exists $h \in H_1$ such that

$$(y_j^{-1}w_j^{-1}t_iw_jy_j)y_j^{-1}\big(w_j^{-1}(y_iw_jy_i^{-1})\big)y_jb_{ij} = ht_{\psi(i,j)}$$

$(i = 1, \dots, s$ and $j = 1, \dots, l)$;

(vi) for $j = l+1, \dots, m$ we have, for all $x \in G_1$, there exists $h \in H_1$ with the property that, for some $i = 1, \dots, s$, there does not exist $h' \in H_1$ such that

$$(y_j^{-1}x^{-1}ht_ixy_j)y_j^{-1}\big(x^{-1}(y_ixy_i^{-1})\big)y_jb_{ij} = h't_{\psi(i,j)};$$

(vii) for $j = 1, \dots, l$, if $x \in G_1$ has the property that, for all $h \in H_1$ and each $i = 1, \dots, s$, there exists $h' \in H_1$ such that

$$(y_j^{-1}x^{-1}ht_ixy_j)y_j^{-1}\big(x^{-1}(y_ixy_i^{-1})\big)y_jb_{ij} = h't_{\psi(i,j)},$$

then there exist $\lambda_1, \dots, \lambda_d \in \mathbb{Z}_p$ such that

$$x = k_1^{\lambda_1} \cdots k_d^{\lambda_d} w_j.$$

Conditions (ii)-(iv) ensure that H is normal in M and conditions (vi) and (vii) ensure that M contains every element that normalizes H. Each of these conditions is definable in $\mathcal{L}_G$; hence, $\zeta^{\mathrm{c}}_{G,p}(s)$ is a rational function in p^{-s}. □

3. Finitely generated groups

Let Γ be a finitely generated group. Then $a_n(\Gamma)$ is finite for all $n \geq 1$. By forming the pro-p-completion $\hat{\Gamma}_p$ of Γ, we may employ the results of the previous sections to deduce rationality results for various Poincaré series associated with Γ. The lemma below is basic and describes how much the pro-p-completion can tell us about subgroups of finite index in Γ.

Let $C(\Gamma)$ be a set of representatives for the conjugacy classes of subgroups of finite index in Γ. Define

$$a_n^{\mathrm{s}}(\Gamma) = \mathrm{card}\{H \leq \Gamma \mid |\Gamma : H| = n \text{ and } H \text{ is subnormal}\},$$
$$a_n^{\lhd}(\Gamma) = \mathrm{card}\{H \leq \Gamma \mid |\Gamma : H| = n \text{ and } H \text{ is normal}\},$$
$$a_n^{\mathrm{cs}}(\Gamma) = \mathrm{card}\{H \in C(\Gamma) \mid |\Gamma : H| = n \text{ and } H \text{ is subnormal}\}.$$

LEMMA 3.1. (i) $a^{\mathrm{s}}_{p^n}(\Gamma) = a_{p^n}(\hat{\Gamma}_p)$;
(ii) $a^{\lhd}_{p^n}(\Gamma) = a^{\lhd}_{p^n}(\hat{\Gamma}_p)$;
(iii) $a^{\mathrm{cs}}_{p^n}(\Gamma) = a^{\mathrm{c}}_{p^n}(\hat{\Gamma}_p)$.

Proof. For part (i) let $G = \hat{\Gamma}_p$. Fix n and let Δ be the intersection of all subnormal subgroups of index p^n in Γ. Then Γ/Δ is a finite p-group, by an elementary argument, so that Γ/Δ is isomorphic to a quotient group of G. Hence $a^{\mathrm{s}}_{p^n}(\Gamma) = a_{p^n}(\Gamma/\Delta) \leq a_{p^n}(G)$. On the other hand, if H denotes the

intersection of all (necessarily open) subgroups of index p^n in G, then G/H is a finite p-group, and so G/H is isomorphic to a quotient of Γ. As every subgroup of G/H is subnormal, this implies that $a_{p^n}(G) \leq a^{\mathrm{s}}_{p^n}(G/H) \leq a^{\mathrm{s}}_{p^n}(\Gamma)$. This proves part (i). Parts (ii) and (iii) follow by the same argument. □

THEOREM 3.2. *Let Γ be a finitely generated group and p a prime. Suppose that $a^{\mathrm{s}}_{p^n}(\Gamma)$ grows at most polynomially with p^n. Then*
(i) $\zeta^{\mathrm{s}}_{\Gamma,p}(s) = \sum_{n\in\mathbb{N}} a^{\mathrm{s}}_{p^n}(\Gamma)p^{-ns}$ *is rational in p^{-s};*
(ii) $\zeta^{\triangleleft}_{\Gamma,p}(s) = \sum_{n\in\mathbb{N}} a^{\triangleleft}_{p^n}(\Gamma)p^{-ns}$ *is rational in p^{-s}; and*
(iii) $\zeta^{\mathrm{cs}}_{\Gamma,p}(s) = \sum_{n\in\mathbb{N}} a^{\mathrm{cs}}_{p^n}(\Gamma)p^{-ns}$ *is rational in p^{-s}.*

Proof. By Lemma 3.1, $a_{p^n}(\hat{\Gamma}_p)$ grows at most polynomially. By [LuM2], Theorem 3.1, or [DxduSMS], Theorem 3.19, $\hat{\Gamma}_p$ is a p-adic analytic pro-p-group. The theorem then follows from Lemma 3.1 and Theorems A, 2.15 and 2.21. □

Parts (ii) and (iii) of the theorem are slightly unsatisfactory, since we would prefer a condition about the growth of $a^{\triangleleft}_{p^n}(\Gamma)$ and $a^{\mathrm{cs}}_{p^n}(\Gamma)$. At present it is still an open problem to characterize pro-p-groups for which $a^{\triangleleft}_{p^n}(G)$ grows polynomially. Such groups include pro-p-groups G of *finite width*, i.e., those pro-p-groups for which there is a bound on the rank of central sections of G. This is a wider class of groups than p-adic analytic groups. For example, the class of analytic groups over $\mathbb{F}_p[[t]]$ has finite width, as does the so-called Nottingham Group (see [Y] for details), a pro-p-group, which is thought not to be analytic in either sense.

Question. Does finite width characterize the class of pro-p-groups for which $a^{\triangleleft}_{p^n}(G)$ grows polynomially?

Let Γ be a finitely generated, residually finite p-group. Then $a^{\mathrm{s}}_{p^n}(\Gamma)$ grows at most polynomially if and only if $\hat{\Gamma}_p$ is a p-adic analytic pro-p-group if and only if there is a bound on the rank of all finite p-quotients of Γ. This class of groups is a subclass of all linear groups over $\mathbb{Z}_p$ (see [DxduSMS], Thm. 6.3). However it is not clear which linear groups are characterized by this condition. For instance, if we consider $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, then Γ contains a residually finite p-subgroup Γ_0 of finite index for which $a^{\mathrm{s}}_{p^n}(\Gamma_0)$ grows faster than polynomially. By Theorem 6.39 of [DxduSMS], the class of groups Γ for which $\hat{\Gamma}_p$ is a p-adic analytic pro-p-group includes the arithmetic groups with the congruence subgroup property and strong approximation. In a sequel [duS2] we shall use Guralnick's classification of subgroups of prime-power index in simple groups (cf. [Gu]) together with Shorey and Tijdeman's work on exponential diophantine equations (cf. [ShT]) to prove that the Poincaré series, counting all subgroups of p-power index in such groups, is rational in p^{-s}. We do this

by identifying a compact p-adic analytic group, whose subgroups of p-power index are in one-to-one correspondence with the subgroups of p-power index inside the arithmetic group.

In the next theorem we describe another class of groups for which we can identify such a compact p-adic analytic group. Recall that

(i) a *chief factor* of Γ is a section M/N, where N is a normal subgroup in Γ and M/N is a minimal normal subgroup of Γ/N, and

(ii) an *upper p-chief factor* of Γ is a chief factor of some finite quotient of Γ, whose order is divisible by p.

THEOREM 3.3. *Let Γ be a finitely generated group and p a prime. Let $\Gamma_0 = \bigcap_S C_\Gamma(S)$, where S ranges over all upper p-chief factors of Γ. Suppose that*

(i) *the orders of all upper p-chief factors of Γ are bounded, and*

(ii) *$a^s_{p^n}(\Gamma_0)$ grows at most polynomially with p^n.*

Then $\zeta_{\Gamma,p}(s)$ is rational in p^{-s}.

Proof. Since the orders of all upper p-chief factors of Γ are bounded and Γ is finitely generated, Γ_0 is a characteristic subgroup of finite index in Γ. Let H be a subgroup of Γ_0 of p-power index. Let K_1 be the largest normal subgroup of Γ contained in H and let K_2 be a normal subgroup such that K_2/K_1 is a chief factor of Γ. Then $K_3 = K_2H \gneqq H$. Since H has p-power index in Γ_0, the order of K_2/K_1 is divisible by p. Thus K_2/K_1 is centralized by Γ_0. This implies that $H \lhd K_3$, since if $k \in K_2$ and $h \in H$, then

$$h^k = h[h,k] \in HK_1 \leq H.$$

Thus, by iterating this argument, we can prove that H is subnormal in Γ_0.

Let $G = \varprojlim_{N \lhd_p \Gamma_0} \Gamma/N$ and $G_0 = \varprojlim_{N \lhd_p \Gamma_0} \Gamma_0/N$. By supposition (ii) and Theorem 3.19 of [DxduSMS], G_0 is an analytic pro-p-group. As G is a finite extension of G_0, it is also a compact p-adic analytic group. The group G has the property that $a_{p^n}(\Gamma) = a_{p^n}(G)$. So Theorem 3.3 follows from Theorem B. □

Definition 3.4. The *upper p-rank* of Γ is defined to be the supremum of $r(P)$ as P ranges over all p-subgroups of finite quotients of Γ.

THEOREM 3.5. *If Γ is a finitely generated group with finite upper p-rank, then $\zeta_{\Gamma,p}(s)$ is rational in p^{-s}.*

Proof. If H is a subgroup of finite index in Γ, then it also has finite upper p-rank. This implies that $a^s_{p^n}(\Gamma_0)$ grows at most polynomially in p^n by the remarks following Theorem 3.2. From Proposition 6.12 of [DxduSMS] there exists a normal subgroup Γ_1 of finite index in Γ with the property that

every finite quotient of Γ_1 has a normal p-complement. (Recall that a *normal p-complement* in a finite group H of order $p^n m$, where $p \nmid m$, is a normal subgroup of H of order m.) It suffices to prove that every upper p-chief factor $S = M/N$ of Γ with $N \leq M \leq \Gamma_1$ has bounded order. Let K/N be a normal p-complement for Γ_1/N. Since $|M/N|$ is divisible by p, $K \cap M \lneq M$. Thus $M^p[M,M] \lneq M$. But $M^p[M,M] \lhd \Gamma$. So M/N is an elementary abelian p-group of bounded rank, since Γ has finite upper p-rank. It follows that the order of all upper p-chief factors of Γ is bounded and, hence, $\zeta_{\Gamma,p}(s)$ is rational in p^{-s} by Theorem 3.3. □

For the class of finitely generated, residually finite groups Γ of finite rank note that $\zeta_{\Gamma,p}(s)$ is rational in p^{-s} for all primes p. This class of groups is precisely the class of finitely generated, residually finite groups for which $a_n(\Gamma)$ grows at most polynomially, namely the class of virtually soluble groups of finite rank (see [LuM1], [LuM2]). However we shall show in [duS2] that there are many groups outside this class for which $\zeta_{\Gamma,p}(s)$ is rational in p^{-s} for all primes p.

ALL SOULS COLLEGE, OXFORD, ENGLAND

REFERENCES

[B] N. BOURBAKI, *Integration*, Fascicules de résultats, Hermann, Paris, 1963.

[D1] J. DENEF, The rationality of the Poincaré series associated to the p-adic points on a variety, Invent. Math. **77** (1984), 1-23.

[D2] ———, On the evaluation of certain p-adic integrals, in *Séminaire de Théorie des Nombres*, Paris, 1983-1984, Progress in Math. **59**, Birkhäuser, 1985, pp. 25-47.

[D3] ———, Multiplicity of the poles of the Poincaré series of a p-adic subanalytic set, in *Séminaire de Théorie des Nombres*, Bordeaux, 1987-1988, Exposé 43, Univ. of Bordeaux I, Talence, 1989.

[DvdD] J. DENEF and L. VAN DEN DRIES, p-adic and real subanalytic sets, Ann. of Math. **128** (1988), 79-138.

[DxduSMS] J.D. DIXON, M.P.F. DU SAUTOY, A. MANN and D. SEGAL, *Analytic Pro-p-Groups*, L.M.S. Lecture Note Series **157**, Cambridge Univ. Press, 1991.

[duS1] M.P.F. DU SAUTOY, Finitely generated groups, p-adic analytic groups and Poincaré series, Bull. A.M.S. **23** (1990), 121-126.

[duS2] ———, Counting congruence subgroups in arithmetic groups, to appear in Bull. L.M.S.

[GSSm] F.J. GRUNEWALD, D. SEGAL and G.C. SMITH, Subgroups of finite index in nilpotent groups, Invent. Math. **93** (1988), 185-223.

[Gu] R.M. GURALNICK, Subgroups of prime power index in a simple group, J. Algebra **81** (1983), 304-311.

[I1] J.-I. IGUSA, Some observations on higher degree characters, Amer. J. of Math. **99** (1977), 393-417.

[I2] ———, *Lectures on Forms of Higher Degree*, Tata Inst. Fund. Research, Bombay, 1978.

[Il] I. ILANI, Zeta functions of $SL(2, \mathbb{Z}_p)$, Preprint.

[L] M. LAZARD, Groupes analytiques p-adiques, I.H.E.S. Publ. Math. **26** (1965), 389-603.

[LuM1] A. LUBOTZKY and A. MANN, Residually finite groups of finite rank, Math. Proc. Cambridge Philos. Soc. **106** (1989), 385-388.

[LuM2] ———, On groups of polynomial subgroup growth, Invent. Math. **104** (1991), 521-533.

[Ma] A. MACINTYRE, On definable subsets of p-adic fields, J. Symb. Logic **41** (1976), 605-610.

[M] A. MANN, Positively finitely generated groups, Preprint.

[ShT] T.N. SHOREY and R. TIJDEMAN, *Exponential Diophantine Equations*, Cambridge Tracts in Math. **87**, Cambridge Univ. Press, 1986.

[vdD] L. VAN DEN DRIES, Analytic Ax–Kochen–Ersov theorems, in *Proceedings of the International Conference on Algebra*, Contemporary Math. **131**, A.M.S., 1992.

[Y] I.O. YORK, *The Group of Formal Power Series under Substitution*, Ph.D. Thesis, Nottingham University, 1990.

(Received September 5, 1991)