ISRAEL JOURNAL OF MATHEMATICS 86 (1994), 1–23

ZETA FUNCTIONS OF GROUPS AND RINGS: UNIFORMITY

BY

MARCUS P.F. DU SAUTOY

All Souls College, Oxford OX1 4AL, England

ABSTRACT

There are various natural local zeta functions associated with groups and rings for each prime p. We consider the question of how these functions behave as we vary the prime p and the groups (or rings) range over a specific class of groups (or rings), e.g. finitely generated torsion-free nilpotent groups of a fixed Hirsch length or p-adic analytic groups of a fixed dimension. Using a result of Macintyre's on the uniformity of parameterized p-adic integrals, together with various natural parameter spaces we define for these classes of groups, we prove a strong finiteness theorem on the possible poles of these local zeta functions.

Notation

$\bar{x}$ denotes an n-tuple $(x_1, \ldots, x_n)$ for some $n \in \mathbf{N}$.

$G^{(n)}$ denotes the direct product of n copies of the group G.

$\mathcal{R}_{d,p}$ denotes the class of rings additively isomorphic to $\mathbf{Z}_p^d$.

$\mathcal{R}_d$ denotes the class of rings additively isomorphic to $\mathbf{Z}^d$.

$\mathcal{T}_{d,p}$ denotes the class of torsion-free finitely generated nilpotent pro-p groups of dimension d.

$\mathcal{T}_d$ denotes the class of torsion-free finitely generated nilpotent groups of Hirsch length d.

$\mathcal{U}_{d,p}$ denotes the class of uniform pro-p groups of dimension d.

$\mathcal{G}_{n,d,p}$ denotes the class of compact p-adic analytic groups containing a d-dimensional normal uniform subgroup of index n.

Received March 9, 1993 and in revised form June 2, 1993

1. Introduction

In [GSS], [duS1] and [duS2], the following zeta functions are defined and considered for a finitely generated abstract or profinite group G:

$$\zeta_G^*(s) = \sum_{H \in \mathcal{X}^*(G)} |G: H|^{-s}$$

where $* \in \{\leq, \triangleleft, \wedge\}$ and

$$\mathcal{X}^{\leq}(G) = \{H \mid H \text{ is a subgroup of finite index in } G\},$$
$$\mathcal{X}^{\triangleleft}(G) = \{H \mid H \text{ is a normal subgroup of finite index in } G\},$$
$$\mathcal{X}^{\wedge}(G) = \{H \mid H \text{ is a subgroup of finite index in } G \text{ and } \hat{H} \cong \hat{G}\};$$

here $\hat{G}$ denotes the profinite completion of G. There are natural "local factors" associated with these zeta functions for each prime p:

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

where $\mathcal{X}_p^*(G) = \{H \in \mathcal{X}^*(G) \mid H \text{ has } p\text{-power index in } G\}$. For the class of finitely generated torsion-free nilpotent groups we can decompose $\zeta_G^*(s)$ as an Euler product of these local factors:

$$\zeta_G^*(s) = \prod_p \zeta_{G,p}^*(s).$$

In [GSS] the rationality of these local factors as functions of p^{-s} was established for nilpotent groups G. Although we cannot hope for a generalization of the Euler product to non-nilpotent groups, in [duS1] and [duS2] the rationality result of [GSS] is extended to p-adic analytic groups G and finitely generated abstract groups of finite rank. These results rely on Denef's application of Macintyre's quantifier elimination for $\mathbf{Z}_p$ to prove the rationality of various p-adic integrals over semi-algebraic sets, and a subsequent extension of this method by Denef and van den Dries to integrals over sub-analytic sets ([D1], [M1] and [DvdD]). In this present paper we shall use a parameterized version of Denef's result together with a result due to Macintyre which allows us to calculate p-adic integrals uniformly for all primes p ([D2] and [M2]) to make some contribution towards the following questions:

QUESTION 1: *For a fixed group G, how does $\zeta^*_{G,p}(s)$ behave as p varies over all primes p?*

QUESTION 2: *For a fixed prime p, how does $\zeta^*_{G,p}(s)$ behave as G varies over p-adic analytic groups of a fixed dimension d (or nilpotent groups of a fixed Hirsch length d)?*

In [GSS] a more specific version of Question 1 was asked for the class of nilpotent groups:

QUESTION 3: *For a fixed finitely generated nilpotent group G do there exist finitely many rational functions $W^*_1(Y,X), \ldots, W^*_n(Y,X)$ of two variables over $\mathbf{Q}$ such that for each prime p there is an i for which $\zeta^*_p(s) = W^*_i(p, p^{-s})$?*

In [GSS] this question is answered affirmatively for free nilpotent groups of class 2. However in a recent paper ([duSL]) more significant progress was made for the function $\zeta^{\wedge}_{G,p}(s)$ in which an affirmative answer to Question 3 is a corollary of an explicit computation of $\zeta^{\wedge}_{G,p}(s)$ in terms of the combinatorial data of $\mathcal{G} = \mathrm{Aut}G$ and representations of $\mathcal{G}$.

There is some hope to develop these combinatorial methods to gain a more explicit hold on the functions $\zeta^{\leq}_{G,p}(s)$ and $\zeta^{\triangleleft}_{G,p}(s)$ but the logical techniques of Denef, van den Dries and Macintyre already give us the following partial answer to Questions 1 and 2:

THEOREM 1: *Let $d \in \mathbf{N}$. There exist $a_i, b_i \in \mathbf{Z}$ ($i = 1, \ldots, h$) such that for each prime p, $* \in \{\leq, \triangleleft, \wedge\}$ and torsion-free finitely generated nilpotent group G of Hirsch length d, there exists a polynomial $\Psi^*_{G,p}(X) \in \mathbf{Q}[X]$ such that*

$$\zeta^*_{G,p}(s) = \frac{\Psi^*_{G,p}(p^{-s})}{\prod_{j \leq h}(1 - p^{-a_j s - b_j})}.$$

The logical techniques therefore give us a very strong finiteness theorem for the poles of our local zeta functions $\zeta^*_{G,p}(s)$ but give us little control on the numerators. If we fix G we can at least bound the degree of $\Psi^*_{G,p}(X)$ as p varies. We have a similar result to Theorem 1 for the class of uniform pro-p groups of dimension d. Using the fact that every compact p-adic analytic group contains a uniform pro-p group of finite index we can extend this to a result about compact p-adic analytic groups at the expense of bounding the index of such a uniform pro-p group.

We begin in §2 by outlining Macintyre's result. In §3 we prove a version of Theorem 1 for zeta functions $\zeta^*_{L,p}(s)$ counting subrings in a ring L additively isomorphic to $\mathbf{Z}^d$ or $\mathbf{Z}_p^d$. To a finitely generated nilpotent group G there is naturally associated a Lie algebra L with the property that for almost all primes p, $\zeta^*_{G,p}(s) = \zeta^*_{L,p}(s)$. We can thus deduce Theorem 1 for almost all primes p as a corollary of results in §3. A similar approach suffices to prove the analogous result for uniform pro-p groups of dimension $d \leq p$. However in §4 we detail a more direct approach to Theorem 1 which spares us having to avoid finitely many primes.

Both the proofs of §3 and §4 depend on defining a natural parameter space $X_d \subseteq \mathbf{Z}_p^n$ for the class of nilpotent groups of Hirsch length d (or rings isomorphic to $\mathbf{Z}^d$ or d-dimensional uniform pro-p groups) with which we can parameterize the integrals defining $\zeta^*_{G,p}(s)$.

We can in fact refine Theorem 1 to prove that the fibres of the natural map from this parameter space X_d to the space of rational functions $\zeta^*_{G,p}(s)$ are definable subsets of $\mathbf{Z}_p^n$.

We observed above that for nilpotent groups we can decompose the global zeta function as an Euler product of the local factors. Unfortunately the lack of control that we presently have on the numerator $\Psi^*_{G,p}(X)$ means that we can infer little about the poles of $\zeta^*_G(s)$ from the results of this present paper.

ACKNOWLEDGEMENT: Part of this work was carried out whilst I was visiting the Institute for Advanced Studies at the Hebrew University of Jerusalem during the year on Field Arithmetic. I should like to thank the Institute for their fantastic hospitality and to thank Alex Lubotzky and Ishai Ilani for discussions whilst I was thinking about this work.

2. Macintyre's Uniformity Theorem

We begin by describing Macintyre's theorem on the uniformity of certain definable p-adic integrals. This theorem will be our basic tool in the remaining sections.

Let $v\colon \mathbf{Q}_p \to \mathbf{Z}\cup\{+\infty\}$ be the valuation on $\mathbf{Q}_p$ with $v(p) = 1$ and let $|\cdot|$ be the normalized absolute value with $|x| = p^{-v(x)}$. Let μ denote the additive Haar measure on $\mathbf{Q}_p$ normalized at $\mathbf{Z}_p$, and also (by abuse of notation) the product measure on free $\mathbf{Z}_p$-modules of the form $\mathbf{Z}_p^m$.

If $A \subseteq \mathbf{Q}_p^{m+k}$ and $\bar{\lambda} \in \mathbf{Q}_p^k$ then we define

$$A(\bar{\lambda}) = \{\bar{x} \in \mathbf{Q}_p^m \mid (\bar{x}, \bar{\lambda}) \in A\}.$$

Let f and g be measurable functions on $\mathbf{Q}_p^{m+k}$ and A a measurable subset of $\mathbf{Q}_p^{m+k}$. Let s be a positive real number.

Definition 2.1:

$$I(f, g, A, \bar{\lambda}, s) = \int_{A(\bar{\lambda})} \mid f(\bar{x}, \bar{\lambda}) \mid^s \mid g(\bar{x}, \bar{\lambda}) \mid d\mu.$$

In [D1] and [D2] Denef proved that $I(f, g, A, \bar{\lambda}, s)$ is a rational function in p^{-s} if A, f and g are definable in some language appropriate for the algebraic theory of $\mathbf{Q}_p$. Here we shall consider A, f and g definable in the language of ring theory L_{RINGS} with $+, =, \cdot, 0, 1$. The formulas defining A, f and g then make sense when realized in $\mathbf{Q}_p$ for all primes p. Macintyre considered the question of how the rational function $I(f, g, A, \bar{\lambda}, s)$ varies with the prime p.

Before we state Macintyre's theorem we recall the definition of a simple function.

Definition 2.2: A function $\theta \colon \mathbf{Q}_p^m \to \mathbf{Z} \cup \{+\infty\}$ is **simple** if there is a finite partition of $\mathbf{Q}_p^m$ into definable subsets A such that for each A there are polynomials $q_1(\bar{x}), q_2(\bar{x}) \in \mathbf{Q}_p[\bar{x}]$, with q_2 non-zero on A, and a positive integer e such that

$$\theta(\bar{x}) = (1/e) v\big(q_1(\bar{x})/q_2(\bar{x})\big),$$

for $\bar{x} \in A$.

For our purpose the following form of Macintyre's result will be sufficient:

PROPOSITION 2.3: *Let A, f and g be definable in L_{RINGS}. Then there exist a_j, $b_j \in \mathbf{Z}$ $(j = 1, \ldots, h)$ such that for each prime p and for all $\bar{\lambda} \in \mathbf{Q}_p^k$ there exists a polynomial $\Psi_{\bar{\lambda},p}(X) \in \mathbf{Q}[X]$ such that*

$$I(f, g, A, \bar{\lambda}, s) = \frac{\Psi_{\bar{\lambda},p}(p^{-s})}{\prod_{j \leq h}(1 - p^{-a_j s - b_j})}.$$

The degree of $\Psi_{\bar{\lambda},p}$ is a simple function in $\bar{\lambda}$. If we fix $\bar{\lambda} \in \mathbf{Z}^k$ then the degree of $\Psi_{\bar{\lambda},p}$ is bounded as p varies.

A more detailed statement of Macintyre's result can be found in §7 of his paper [M2] where some control on the nature of the numerator is detailed but not such as to be useful in our context. The proof of Macintyre's theorem relies on a uniform approach to quantifier elimination for $\mathbf{Q}_p$ and a uniform Cell-Decomposition Theorem. As we shall only be plundering the results at this stage we need go no further into the proof of this theorem but rather refer the interested reader to Macintyre's paper. We should also make reference to the work of Pas who proved a similar uniformity result to Macintyre's (see [P1] and [P2]).

In a subsequent paper we analyse the proof of Proposition 2.3 in order to show that some sort of progress can be made for integrals defined in the ring $\mathbf{F}_p[[t]]$. This will have implications for counting subgroups and subalgebras in Lie groups and algebras over $\mathbf{F}_p[[t]]$.

3. Zeta functions associated to rings

Let L be a not necessarily associative ring and p a prime. Define

$$\zeta^*_{L,p}(s) = \sum_{H \in \mathcal{X}^*_p(L)} |\, L\colon H\,|^{-s}$$

where $* \in \{\leq, \triangleleft, \wedge\}$ and

$$\mathcal{X}^{\leq}_p(L) = \{H \mid H \text{ is a subring of } p\text{-power index in } L\},$$
$$\mathcal{X}^{\triangleleft}_p(L) = \{H \mid H \text{ is an ideal of } p\text{-power index in } L\},$$
$$\mathcal{X}^{\wedge}_p(L) = \{H \mid H \in \mathcal{X}^{\leq}_p(L) \text{ and } \hat{H} \cong \hat{L}\}.$$

Let $\mathcal{R}_{d,p}$ be the class of rings L additively isomorphic to $\mathbf{Z}_p^d$. We define a natural moduli space for $\mathcal{R}_{d,p}$. To each $L \in \mathcal{R}_{d,p}$ associate the subset $A(L) \subseteq (\mathrm{M}_d(\mathbf{Z}_p))^d = \mathbf{Z}_p^{d^3}$ defined by:

$$A(L) = \left\{ \begin{array}{r} ((a_{ij1}),\ldots,(a_{ijd})) \mid \text{there exists a basis } e_1,\ldots,e_d \text{ of } L \\ \text{such that } e_i.e_j = \sum_{k=1}^{d} a_{ijk}e_k. \end{array} \right\}$$

Let $W_{d,p} = \bigcup_{L\in\mathcal{R}_{d,p}} A(L)$. $W_{d,p}$ is an algebraic subvariety of $\mathbf{Z}_p^{d^3}$. The group $\mathrm{GL}_d(\mathbf{Z}_p)$ has a natural action on $W_{d,p}$ via $((a_{ij1}),\ldots,(a_{ijd}))g = ((b_{ij1}),\ldots,(b_{ijd}))$ where $b_{ijk} = \sum g_{il}g_{jm}a_{lmn}(g^{-1})_{nk}$. It is easy to see that the orbits of $\mathrm{GL}_d(\mathbf{Z}_p)$ correspond to isomorphism classes of $\mathbf{Z}_p$-rings. Let $\mathcal{L}_{d,p}$ be the subclass of $\mathcal{R}_{d,p}$ consisting of those rings which have the structure of a Lie algebra. The subset

$V_{d,p} = \bigcup_{L \in \mathcal{L}_{d,p}} A(L)$ is a subvariety of $W_{d,p}$ since the fact that $\big((a_{ij1}), ..., (a_{ijd})\big)$ are structure constants for a Lie algebra is defined by polynomial conditions in a_{ijk}. In the next section we will see that $V_{d,p}$ is a parameter space for the class of d-dimensional uniform pro-p groups.

We raise the following natural questions (cf. [GS]):

QUESTION 3.1: *Describe the algebraic varieties $W_{d,p}$ and $V_{d,p}$. What are their irreducible components? What are their dimensions? Are the different irreducible components definable by structural conditions on the corresponding rings or Lie algebras?*

Rather than concentrating on these questions, we turn to the task of using the variety $W_{d,p}$ to parameterize the integrals defining $\zeta^*_{L,p}(s)$. We define subsets M^*_p of $\mathrm{Tr}_d(\mathbf{Z}_p) \times \mathbf{Z}_p^{d^3}$ for each $* \in \{\leq, \triangleleft, \wedge\}$. If $\big((m_{ij}), (a_{ij1}), ..., (a_{ijd})\big) \in \mathrm{Tr}_d(\mathbf{Z}_p) \times \mathbf{Z}_p^{d^3}$ then we let $\bar{m}_i$ denote the ith row of (m_{ij}), $\bar{m}_i^t$ its transpose and $A_l = (a_{ijl})$.

(1) Let $M_p^{\leq}$ be the set of $\big((m_{ij}), (a_{ij1}), ..., (a_{ijd})\big)$ satisfying:

$$\text{for } 1 \leq i, j \leq d \; \exists \; Y_{ij}^1, ..., Y_{ij}^d \in \mathbf{Z}_p \text{ such that}$$
$$\bar{m}_i A_l \bar{m}_j^t = \sum_{k=1}^{d} Y_{ij}^k m_{kl} \quad \text{for } l = 1, ..., d.$$

(2) Let $M_p^{\triangleleft}$ be the set of $\big((m_{ij}), (a_{ij1}), ..., (a_{ijd})\big)$ satisfying:

$$\text{for } 1 \leq i, j, \leq d \; \exists \; Y_{ij}^1, ..., Y_{ij}^d \in \mathbf{Z}_p \text{ such that}$$
$$\sum_{k=1}^{d} m_{ik} a_{kjl} = \sum_{k=1}^{d} Y_{ij}^k m_{kl} \quad \text{for } l = 1, ..., d.$$

(3) Let $M_p^{\wedge}$ be the set of $\big((m_{ij}), (a_{ij1}), ..., (a_{ijd})\big)$ satisfying:

$$\text{for } 1 \leq i, j \leq d \; \exists \; Y_{ij}, Z_{ij} \in \mathbf{Z}_p \text{ such that}$$
$$\text{if } \bar{n}_i = \sum_{j=1}^{d} Z_{ij} \bar{m}_j \text{ then for each } 1 \leq i, j, r \leq d$$
$$\bar{m}_i = \sum Y_{ij} \bar{n}_j \quad \text{and} \quad \sum_{k,l=1}^{d} Z_{ik} Z_{jl} \bar{m}_k A_r \bar{m}_l^t = \sum_{k=1}^{d} a_{ijk} n_{kr}.$$

If $\bar{a} = \big((a_{ij1}), \ldots, (a_{ijd})\big) \in A(L)$ then, setting $f = m_{11} m_{22} \cdots m_{nn}$ and $g = m_{11} m_{22}^2 \cdots m_{nn}^n$,

$$\zeta^*_{L,p}(s) = I(f, g, M^*_p, \bar{a}, s).$$

An explanation of why this is true for $* \in \{\leq, \triangleleft\}$ may be found in §3 of [GSS]. For $* = \wedge$, it is an easy exercise to adapt the proof of Proposition 2.7 of the same paper [GSS]. Thus $W_{d,p}$ parameterizes the integrals describing the functions $\{\zeta^*_{L,p}(s) \mid L \in \mathcal{R}_{d,p}\}$. Now the subsets M^*_p and functions f and g are definable in L_{RINGS} and the formula defining M^*_p is independent of the prime p. We can therefore immediately apply Macintyre's theorem of §2 to deduce:

THEOREM 3.2: *Let $d \in \mathbf{N}$. There exist $a_j, b_j \in \mathbf{Z}$ $(j = 1, ..., h)$ such that for each prime p, $* \in \{\leq, \triangleleft, \wedge\}$ and $L \in \mathcal{R}_{d,p}$ there exists a polynomial $\Psi^*_{L,p}(X) \in \mathbf{Q}[X]$ such that*

$$\zeta^*_{L,p}(s) = \frac{\Psi^*_{L,p}(p^{-s})}{\prod_{j \leq h}(1 - p^{-a_j s - b_j})}.$$

Let $\mathcal{R}_d$ denote the class of rings L additively isomorphic to $\mathbf{Z}^d$.

COROLLARY 3.3: *There exist $a_j, b_j \in \mathbf{Z}$ $(j = 1, ..., h)$ such that for each $L \in \mathcal{R}_d$, prime p and $* \in \{\leq, \triangleleft, \wedge\}$ there exists a polynomial $\Psi^*_{L,p}(X) \in \mathbf{Q}[X]$ such that*

$$\zeta^*_{L,p}(s) = \frac{\Psi^*_{L,p}(p^{-s})}{\prod_{j \leq h}(1 - p^{-a_j s - b_j})}.$$

If we fix $L \in \mathcal{R}_d$ then $\deg \Psi^*_{L,p}(X)$ is bounded as p varies.

Proof: The first part follows from the fact that

$$\zeta^*_{L,p}(s) = \zeta^*_{L \otimes \mathbf{Z}_p, p}(s).$$

The bound on deg $\Psi^*_{L,p}(s)$ (which had already been established in [GSS]) follows from the last statement of Proposition 2.3 since there exists $\bar{a} \in \mathbf{Z}^{d^3}$ such that $\bar{a} \in A(L \otimes \mathbf{Z}_p)$ for all primes p. ∎

There is a natural topology on $W_{d,p}$ inherited from the topology on $\mathbf{Z}_p^{d^3}$. If we give the set $\mathcal{R}_{d,p}$ the structure of a topological space by defining open neighbourhoods of a point $L \in \mathcal{R}_{d,p}$ by $U_{L,N} = \{L' \mid L/p^N L \cong L'/p^N L'\}$ for $N \in \mathbf{N}$, then the natural map

$$\Phi \colon W_{d,p} \longrightarrow \mathcal{R}_{d,p}$$

is continuous. Define the topology on the set of power series $\mathbf{Q}[[X]]$ via the metric $d(F(X), G(X)) = p^{-\partial(F(X)-G(X))}$ where $\partial(\sum_{n=0}^{\infty} a_n x^n) = m$ if $a_n = 0$ for $m > n$ and $a_m \neq 0$. Then it is clear that the map $Z^* \colon \mathcal{R}_{d,p} \to \mathbf{Q}[[X]]$ defined by $L \longmapsto \zeta^*_{L,p}(s)$ is continuous. Note that since the image of Z^* is contained in the set of all rational functions, a countable subset of the set of all power series, we have by cardinality considerations that, since $\mathcal{R}_{d,p}$ is uncountable, there are uncountably many rings with the same zeta function $\zeta^*_{L,p}(s)$. In fact the fibres of this map are definable subsets of $W_{d,p}$:

THEOREM 3.4: *We can partition $W_{d,p}$ into countably many definable subsets $\{A_i \mid i \in I\}$ on which $Z^* \circ \Phi$ is constant.*

Proof: The function $\theta^*\colon W_{d,p} \to \mathbf{Z} \cup \{+\infty\}$ defined by

$$\bar{a} \mapsto \deg \Psi^*_{\Phi(\bar{a}),p}(X)$$

is a simple function by Macintyre's theorem, Proposition 2.3. So there exists a finite partition of $\mathbf{Z}_p^{d^3}$ into definable subsets A such that for each A there are polynomials $q_1(\bar{x}), q_2(\bar{x}) \in \mathbf{Q}_p[\bar{x}]$ with q_2 non-zero on A, and a positive integer e such that

$$\theta^*(\bar{a}) = (1/e)v\big(q_1(\bar{a})/q_2(\bar{a})\big)$$

for $\bar{a} \in A$.

Let $\bar{a} \in A \cap W_{d,p}$. There is a neighbourhood $\bar{a} + p^n\mathbf{Z}_p^{d^3}$ of $\bar{a}$ such that if $\bar{b} \in A \cap (\bar{a} + p^n\mathbf{Z}_p^{d^3})$ then

$$\theta^*(\bar{b}) = \theta^*(\bar{a}).$$

This follows from the fact that (i) if $q(\bar{x}) = \sum_{\bar{\alpha}\in\mathbf{N}^{d^3}} c_{\bar{\alpha}} x_1^{\alpha_1} \cdots x_{d^3}^{\alpha_{d^3}} \in \mathbf{Q}_p[\bar{x}], v(c_{\bar{\alpha}}) > r_1$ for all $\bar{\alpha} \in \mathbf{N}^{d^3}$ and $v\big(q(\bar{a})\big) = r_2$ then $v\big(q(\bar{a} + p^{r_2 - r_1}\mathbf{Z}_p^{d^3})\big) = r_2$ and (ii) $v\big(q_1(\bar{a})/q_2(\bar{a})\big) = v\big(q_1(\bar{a})\big) - v\big(q_2(\bar{a})\big)$.

Suppose now that L and $L' \in \mathcal{R}_{d,p}$ and that $\deg\Psi^*_{L,p}(X), \deg\Psi^*_{L',p}(X) \leq m$. Let $a^*_{p^n}(L) = \operatorname{card}\{H \in \mathcal{X}^*_p(L) \mid\mid L\colon H \mid= p^n\}$. The ith coefficient of $\Psi^*_{L,p}(X)$ is determined by $a^*_{p^n}(L)$ for $n \leq i$. Thus $L/p^mL \cong L'/p^mL'$ implies that $\Psi^*_{L,p}(X) = \Psi^*_{L',p}(X)$ since

$$a^*_{p^i}(L) = a^*_{p^i}(L/p^mL) = a^*_{p^i}(L'/p^mL') = a^*_{p^i}(L')$$

for $i \leq m$.

If $\bar{b} \in \bar{a} + p^m\mathbf{Z}_p^{d^3}$ then the ring $\Phi(\bar{b})$ has the property that $\Phi(\bar{b})/p^m\Phi(\bar{b}) \cong \Phi(\bar{a})/p^m\Phi(\bar{a})$. Therefore the function $Z^* \circ \Phi$ is constant on $A \cap W_{d,p} \cap (\bar{a} + p^r\mathbf{Z}_p^{d^3})$ where $r = \max\{n, \theta^*(\bar{a})\}$. This completes the proof of Theorem 3.4. ∎

We can in fact use the structure of definable sets provided by Macintyre's quantifier elimination for $\mathbf{Z}_p$ to give another interpretation of Theorem 3.4. If A is definable then, by quantifier elimination, A is a finite union of sets of the $X \cap Y$ where X is open and Y is the zero-set of a polynomial (see [M1]). So we have countably many polynomials f such that on each subvariety $W_{d,p}(f)$ of $W_{d,p}$ defined by

$$W_{d,p}(f) = \{\bar{a} \in W_{d,p} \mid f(\bar{a}) = 0\}$$

$Z^* \circ \Phi$ is locally constant.

We end this section by raising some questions of a related nature. It is natural to ask how the zeta function of a subring of L relates to that of L. Surprisingly little is known about this question even if we restrict ourselves to subrings of the form $p^n L$. Define the injective map

$$\triangle_p\colon \mathcal{R}_{d,p} \longrightarrow \mathcal{R}_{d,p}$$

by $L \mapsto pL$.

QUESTION 3.5: *How do the zeta functions behave under the map $\triangle_p$?*

For $d = 3$ it is a straightforward exercise to prove:

LEMMA 3.6:

$$\zeta_{\mathbf{Z}_p^3,p}(s) - \zeta^*_{pL,p}(s) = p^{-(2s-2)}\big(\zeta_{\mathbf{Z}_p^3,p}(s) - \zeta^*_{L,p}(s)\big).$$

Can we generalize Lemma 3.6 to larger dimensions? Notice that the degree of the polynomials $\Psi^*_{p^nL,p}(X)$ increases as $n \to \infty$. This hints perhaps at a natural partition of $W_{d,p}$ and $\mathcal{R}_{d,p}$ which would provide a better setting in which to refine Theorem 3.4. To describe this partition we make the following:

Definition 3.7: We define a ring $L \in \mathcal{R}_{d,p}$ to be **powerful of order** k if p is odd and $p^k L \geq L^2$ but $p^{k+1}L \not\geq L^2$ or $p = 2$ and $2^{k+1}L \geq L^2$ but $2^{k+2}L \not\geq L^2$. L is **powerful of order** ∞ if $p^k L \geq L^2$ for all k.

Note that our usual definition of powerful now corresponds to the concept of powerful of order $k \geq 1$. If L is powerful of order k then $p^l L$ is powerful of order $l + k$.

We partition $\mathcal{R}_{d,p}$ into subsets $\mathcal{R}_{d,p,k}$ consisting of powerful rings L of order k. The map $\triangle_p$ restricts to a bijective map

$$\triangle_p\colon \mathcal{R}_{d,p,k} \longrightarrow \mathcal{R}_{d,p,k+1}.$$

Let $W_{d,p,k} = \Phi^{-1}(\mathcal{R}_{d,p,k})$ then $W_{d,p,k}$ is certainly definable since

$$\text{for } p \text{ odd} \quad W_{d,p,k} = W_{d,p} \cap p^k \mathbf{Z}_p^{d^3} \smallsetminus p^{k+1}\mathbf{Z}_p^{d^3},$$
$$\text{for } p = 2 \quad W_{d,2,k} = W_{d,2} \cup 2^{k+1}\mathbf{Z}_2^{d^3} \smallsetminus 2^{k+2}\mathbf{Z}_2^{d^3}.$$

QUESTION 3.8: *How does $\Psi^*_{L,p}(X)$ behave on $\mathcal{R}_{d,p,k}$ for fixed k? In the light of Theorem 3.4, might the degree of $\Psi^*_{L,p}(X)$ be bounded on $\mathcal{R}_{d,p,k}$? Is Z^* finite valued on $\mathcal{R}_{d,p,k}$?*

4. Zeta functions associated to groups

There are various classes of groups which have Lie algebras associated to them in such a way that there is a one-to-one correspondence between subgroups and subalgebras. In these settings we can deduce the uniformity results of the previous section for the zeta functions associated with groups defined in the introduction.

Let G be a torsion-free, finitely generated nilpotent group. Associated with G there is a Lie algebra $L_G(\mathbf{Q})$ over $\mathbf{Q}$ of dimension equal to the Hirsch length $h(G)$ of G. There is an injective mapping log: $G \to L_G(\mathbf{Q})$ such that the set $\log G$ spans $L_G(\mathbf{Q})$ (see [S1], Chapter 6 or [GS]). In general, $\log G$ will not be an additive subgroup of $L_G(\mathbf{Q})$. However in [GSS] the following result is established:

PROPOSITION 4.1: *Let $\mathcal{T}_d$ denote the class of torsion-free finitely generated nilpotent groups of Hirsch length d. Then there exists $f \in \mathbf{N}$ depending only on d such that if $G \in \mathcal{T}_d$ then $L = \log G^f$ is a Lie subring of $L_G(\mathbf{Q})$ and*

$$\zeta^*_{G,p}(s) = \zeta^*_{L,p}(s)$$

for $* \in \{\leq, \triangleleft, \wedge\}$ and all primes p not dividing f.

This theorem gives us an immediate corollary to Corollary 3.3 where we replace $\mathcal{R}_d$ by $\mathcal{T}_d$ but restrict ourselves to p not dividing f. However we can do better than this by directly parameterizing the integrals defined in [GSS] describing $\zeta^*_{G,p}(s)$.

Let G be a finitely generated torsion-free nilpotent pro-p group. Fix a Mal'cev basis $(x_1, ..., x_d)$ for G. G may then be identified with the set of all p-adic words of the form

$$x(\bar{a}) = x_1^{a_1} \cdots x_d^{a_d}$$

with $\bar{a} = (a_1, ..., a_d) \in \mathbf{Z}_p^d$. There exist polynomials over $\mathbf{Q}_p$ defining

$$\lambda\colon \mathbf{Z}_p^d \times \mathbf{Z}_p \to \mathbf{Z}_p^d,$$
$$\mu\colon \mathbf{Z}_p^d \times \mathbf{Z}_p^d \to \mathbf{Z}_p^d,$$

such that for $\bar{a}, \bar{b} \in \mathbf{Z}_p^d$ and $k \in \mathbf{Z}_p$

$$x(\bar{a})^k = x\big(\lambda(\bar{a}, k)\big),$$
$$x(\bar{a}).x(\bar{b}) = x\big(\mu(\bar{a}, \bar{b})\big).$$

The existence of such polynomials was first proved by P. Hall [H]. In order to parameterize the zeta functions $\zeta^*_{G,p}(s)$ we need to analyse Hall's proof to establish the following:

Lemma 4.2: *Let $\mathcal{T}_{d,p}$ denote the class of torsion-free finitely generated nilpotent pro-p groups of dimension d. There is a bound $N(d)$, depending only on d, such that for $G \in \mathcal{T}_{d,p}$, the polynomials $\lambda = (\lambda_1, \ldots, \lambda_d)$ and $\mu = (\mu_1, \ldots, \mu_d)$ have degree bounded by $N(d)$.*

Proof: We proceed by induction on the dimension d. For $d = 1$, we have $N(1) = 2$. Suppose that the lemma is true for nilpotent pro-p groups of dimension $< d$ and that the degree of the polynomials defining multiplication and exponentiation in $G \in \mathcal{T}_{i,p}$ for $i = 1, \ldots, d-1$ is bounded by $\alpha(d)$. Let $G \in \mathcal{T}_{d,p}$. Then, for $\bar{a}, \bar{b} \in \mathbf{Z}_p^d$,

$$\begin{aligned} x\big(\mu(\bar{a}, \bar{b})\big) &= x(\bar{a}).x(\bar{b}) \\ &= x_1^{a_1+b_1} \prod_{i=2}^{d} (x_1^{-b_1} x_i^{-1} x_1^{b_1})^{a_i} x_2^{b_2} \cdots x_d^{b_d}. \end{aligned} \tag{1}$$

Now

$$x_1^{-b_1} x_i^{-1} x_1^{b_1} = x_1^{-b_1} (x_i^{-1} x_1 x_i)^{b_1} x_i^{-1}$$
$$\text{and } x_i^{-1} x_1 x_i = x_1 x_{i+1}^{c_{i,1}} \cdots x_d^{c_{i,d-i}}$$

where $c_{i,j} \in \mathbf{Z}_p$ since $G_i = \{x_i^{a_i} \cdots x_d^{a_d} \mid a_i, \ldots, a_d \in \mathbf{Z}_p\}$ is a central series in G. Set $N_i = \{x_1^{a_1} x_{i+1}^{a_{i+1}} \cdots x_d^{a_d} \mid a_1, a_{i+1}, \ldots, a_d \in \mathbf{Z}_p\}$ for $i = 2, \ldots, d-1$. N_i has a Mal'cev basis $(x_1, x_{i+1}, \ldots, x_d)$. Applying our inductive hypothesis to N_i

$$(x_i^{-1} x_1 x_i)^{b_1} = x_1^{b_1} x_{i+1}^{\varphi_{i,1}} \cdots x_d^{\varphi_{i,d-i}}$$

where the $\varphi_{i,j}$ are polynomials in b_1 of degree bounded by $\alpha(d)$. So

$$x_1^{-b_1}x_i^{-1}x_1^{b_1} = x_i^{-1}x_{i+1}^{\psi_{i,1}}\cdots x_d^{\psi_{i,d-i}}$$

where the $\psi_{i,j}$ are polynomials in b_1 of degree bounded by $\big(\alpha(d)\big)^2$. Hence

$$(x_1^{-b_1}x_i^{-1}x_1^{b_1})^{-a_i} = x_i^{a_i}x_{i+1}^{\theta_{i,1}}\cdots x_d^{\theta_{i,d-i}}$$

where the $\theta_{i,j}$ are polynomials in b_1 and a_i of degree bounded by $\big(\alpha(d)\big)^3$. Substituting the above into (1) and applying our inductive hypothesis to G_2 we can deduce that μ is bounded in degree by $\big(\alpha(d)\big)^{d+2}$. Set $\beta(d) = \big(\alpha(d)\big)^{d+2}$.

We now turn to bounding the degree of λ. Let $v_i = \tau_i(x_1^{a_1}, ..., x_d^{a_d})$ where $\tau_i(\bar{y})$ is the ith Petresco word defined by

$$y_1^i \cdots y_d^i = \tau_1(\bar{y})^i \cdots \tau_k(\bar{y})^{\binom{i}{k}} \cdots \tau_i(\bar{y}).$$

An inductive argument on i together with the bound $\beta(d)$ on the degree of μ suffices to establish a bound $\gamma(d)$ on the degree of polynomials $w_{i,j}$ $(i, j \leq d)$ defining the coordinates of v_i:

$$v_i = x_1^{w_{i,1}} \cdots x_d^{w_{i,d}}.$$

Since $v_i \in \gamma_i(G)$, the ith term of the lower central series of G and G has class $\leq d, v_i = 1$ for $i \geq d$. So

$$x\big(\lambda(\bar{a}, k)\big) = v_1^k = x(k.\bar{a}).v_d^{-\binom{k}{d}} \cdots v_2^{-\binom{k}{2}}.$$

Since $\gamma_i(G)$ has dimension $< d$, the coordinates of $v_i^{-\binom{k}{i}}$ are defined by polynomials of degree bounded by $\gamma(d).i.\alpha(d)$. Hence the degree of λ is bounded by $\gamma(d).d.\alpha(d).\beta(d)^{k-1}$. This completes the proof of Lemma 4.2. ∎

We can now define generic polynomials which when specialized define multiplication and exponentiation in $G \in \mathcal{T}_{d,p}$. Let $I = \{0, ..., N(d)\}$ and

$$\Lambda\big(X_1, ..., X_d, Y, C_{\bar{\alpha}}; \bar{\alpha} \in I^{d+1}\big) = \sum_{\bar{\alpha} \in I^{d+1}} C_{\bar{\alpha}} X_1^{\alpha_1} \cdots X_d^{\alpha_d} Y^{\alpha_{d+1}}$$

$$M\big(X_1, ..., X_d, Y_1, ..., Y_d, D_{\bar{\alpha},\bar{\beta}}; \bar{\alpha}, \bar{\beta} \in I^d\big) = \sum_{\bar{\alpha},\bar{\beta} \in I^d} D_{\bar{\alpha},\bar{\beta}} X_1^{\alpha_1} \cdots X_d^{\alpha_d} Y_1^{\beta_1} \cdots Y_d^{\beta_d}.$$

Then, for each $G \in \mathcal{T}_{d,p}$, there exist $c_{\bar{\alpha}}(G), d_{\bar{\alpha},\bar{\beta}}(G) \in \mathbf{Q}_p$ such that

$$\lambda(\bar{a}, k) = \Lambda(\bar{a}, k, c_{\bar{\alpha}}(G)),$$
$$\mu(\bar{a}, \bar{b}) = M(\bar{a}, \bar{b}, d_{\bar{\alpha},\bar{\beta}}(G)).$$

In [GSS] §2, for each $G \in \mathcal{T}_{d,p}$ subsets definable in L_{RINGS} $M^*_{G,p} \subseteq \mathbf{Z}_p^{d(d-1)/2} = \mathrm{Tr}_d(\mathbf{Z}_p)$, $* \in \{\leq, \triangleleft, \wedge\}$, are constructed such that

$$\zeta^*_{G,p}(s) = \int_{M^*_{G,p}} | m_{11} |^{s-1} \cdots | m_{dd} |^{s-d} \, d\mu.$$

We refer the reader to the paper [GSS] for the precise defining conditions for the subsets $M^*_{G,p}$ which are similar in character to those defined in §3 of this paper for rings. In a similar fashion to the formulas for rings, we can then define formulas $\Psi^*(X_{ij}, C_{\bar{\alpha}}, D_{\bar{\alpha},\bar{\beta}})$ in the polynomials $\Lambda(X_1, ..., X_d, Y, C_{\bar{\alpha}})$ and $M(X_1, ..., X_d, Y_1, ..., Y_d, D_{\bar{\alpha},\bar{\beta}})$ such that for each $G \in \mathcal{T}_{d,p}$

$$\begin{aligned} M^*_{G,p} &= \left\{ (m_{ij}) \in \mathbf{Z}_p^{d(d-1)/2} \mid \Psi^*\big(m_{ij}, c_{\bar{\alpha}}(G), d_{\bar{\alpha},\bar{\beta}}(G)\big) \text{ is true in } \mathbf{Z}_p \right\} \\ &= A^*\big(c_{\bar{\alpha}}(G), d_{\bar{\alpha},\bar{\beta}}(G)\big). \end{aligned}$$

Thus the integrals

$$\int_{A^*\left(c_{\bar{\alpha}}(G), d_{\bar{\alpha},\bar{\beta}}(G)\right)} | m_{11} |^{s-1} \cdots | m_{dd} |^{s-d} \, d\mu$$

parameterize all the zeta functions $\zeta^*_{G,p}(s)$ for $G \in \mathcal{T}_{d,p}$ and p prime. Macintyre's theorem therefore gives us an analogous result for nilpotent groups to the uniformity results of §3.

THEOREM 4.3: *Let $d \in \mathbf{N}$. There exist $a_j, b_j \in \mathbf{Z}$ ($j = 1, ..., h$) such that for each prime p, $* \in \{\leq, \triangleleft, \wedge\}$ and $G \in \mathcal{T}_{d,p}$ there exists a polynomial $\Psi^*_{G,p}(X) \in \mathbf{Q}[X]$ such that*

$$\zeta^*_{G,p}(s) = \frac{\Psi^*_{G,p}(p^{-s})}{\prod_{j \leq h}(1 - p^{-a_j s - b_j})}.$$

If $G \in \mathcal{T}_d$ then, since $\zeta^*_{G,p}(s) = \zeta^*_{\hat{G}_p,p}(s)$ (where $\hat{G}_p$ denotes the pro-p completion of G), we get the same result for $\mathcal{T}_d$ as in Corollary 3.3. This establishes Theorem 1 of the Introduction. If we fix $G \in \mathcal{T}_d$ then deg $\Psi^*_{G,p}(X)$ is bounded as p varies. The bound on the degrees of the rational functions $\zeta^*_{G,p}(s)$ as p varies had already been established in [GSS] using Macintyre's theorem. This bound was applied to Question 3 posed in the Introduction to establish an affirmative answer for $\zeta^*_{F,p}(s)$ where F is the free nilpotent group of class 2.

As we mentioned in the Introduction, the rationality of $\zeta^*_{G,p}(s)$ can be generalized to the class of compact p-adic analytic groups. But here we make use of the rationality of integrals definable not in L_{RINGS} but the language describing the analytic theory of $\mathbf{Q}_p$, L_{AN}, proved by Denef and van den Dries (see [DvdD]). As yet, no analogue of Macintyre's result exists for the analytic theory of $\mathbf{Q}_p$ as p varies. However there is a certain setting in which, as for nilpotent groups, there exists a Lie algebra associated with an analytic group G whose subalgebras are in one-to-one correspondence with subgroups of G.

Definition 4.4: G is a **uniform pro-p group** if (1) G is (topologically) finitely generated, (2) G is powerful (i.e. $G^p \geq [G,G]$ if $p > 2$ and $G^4 \geq [G,G]$ if $p = 2$) and (3) G is torsion-free.

We refer the reader to [DduSMS] for details about uniform pro-p groups. In particular, to a uniform pro-p group G there is naturally associated a Lie algebra $L(G)$ which is defined by the following intrinsic Lie algebra operations that exist on the group G:

$$g + h = \lim_{n\to\infty}(g^{p^n}h^{p^n})^{p^{-n}},$$
$$(g,h) = \lim_{n\to\infty}[g^{p^n}, h^{p^n}]^{p^{-2n}},$$
$$\lambda.g = g^{\lambda},$$

where $g, h \in G$ and $\lambda \in \mathbf{Z}_p$. This Lie algebra $L(G)$ has the following properties, the first of which was established by Ilani [I]:

PROPOSITION 4.5: *Let G be a uniform pro-p group.*

(i) *If G has dimension $d(G) \leq p$ then*

$$\zeta^*_{G,p}(s) = \zeta^*_{L(G),p}(s)$$

for $* \in \{\leq, \triangleleft\}$.

(ii) *For all primes p*

$$\zeta^{\wedge}_{G,p}(s) = \zeta^{\wedge}_{L(G),p}(s).$$

Proof: We prove (ii) since the details of (i) can be found in [I]. The subtlety of (i) arises from the fact that if $H \leq G$ then in general H need not be closed under the intrinsic Lie operations on G. The condition of (i) on the dimension enables Ilani to show in fact that this subset is closed under the Lie algebra operations and conversely that any Lie subalgebra of $L(G)$ is the image of some subgroup H. However in the situation of part (ii) we need only consider subgroups H isomorphic to G (and similarly for subalgebras of $L(G)$) since for a pro-p group $\hat{H} \cong \hat{G}$ if and only if $H \cong G$. The subgroup H is therefore uniform and hence the intrinsic Lie algebra operations on G restrict to the intrinsic Lie operations defined on H as a uniform group. The fact that these Lie algebras are isomorphic then follows immediately from the isomorphism (which is a continuous map) of G and H as uniform groups.

Conversely, as outlined in [I], if H is a uniform Lie subalgebra of $L(G)$ then it is a subgroup of G since it is closed under the Baker-Campbell-Hausdorff series which defines the group operation on G. Again H will be isomorphic to G as a subgroup if H is isomorphic to $L(G)$ as a subalgebra since the group operation on H is determined by the structure of H as a Lie algebra.

Thus we have a one-to-one correspondence between subgroups of G isomorphic to G and subalgebras of $L(G)$ isomorphic to $L(G)$; that the correspondence is index-preserving follows from [DduSMS] Corollary 4.15. This completes the proof of (ii). ∎

For $\zeta^{\wedge}_{G,p}(s)$ this immediately gives us an analogue of Theorem 4.3 where we substitute for $\mathcal{T}_{d,p}$ the class $\mathcal{U}_{d,p}$ of uniform pro-p groups of dimension d. But for $\zeta^{\leq}_{G,p}(s)$ and $\zeta^{\triangleleft}_{G,p}(s)$ we must restrict ourselves to primes $p \geq d$. However we can recover those primes $p < d$ because, although we do not have the uniformity result of Macintyre, we now only have to consider a finite number of primes and for p fixed we do have a parameterized version of Denef and van den Dries's result in the analytic language L_{AN}. Recall that L_{AN} is the language having for each $n \in \mathbf{N}$ and each power series

$$f \in \left\{ \sum_{\bar{\alpha} \in \mathbf{N}^n} a_{\bar{\alpha}} X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in \mathbf{Z}_p[[\bar{X}]] \mid a_{\bar{\alpha}} \to 0 \text{ as } \alpha_1 + \cdots + \alpha_n \to \infty \right\}$$

an n-ary function symbol f to be interpreted as the corresponding function $\mathbf{Z}_p^n \to \mathbf{Z}_p$.

THEOREM 4.6: *Let p be a prime and $A \subseteq \mathbf{Q}_p^{m+k}$, $f, g\colon \mathbf{Q}_p^{m+k} \to \mathbf{Q}_p$ be definable in L_{AN}. There exist $a_j, b_j \in \mathbf{Z}$ $(j = 1, ..., h)$ such that for all $\bar{\lambda} \in \mathbf{Q}_p^k$ there exists a polynomial $\Psi_{\bar{\lambda}}(X) \in \mathbf{Q}[X]$ such that*

$$I(f, g, A, \bar{\lambda}, s) = \frac{\Psi_{\bar{\lambda}}(p^{-s})}{\prod_{j \leq h}(1 - p^{-a_j s - b_j})}.$$

Proof: Denef's proof in the algebraic language L_{RINGS} was a consequence of the proof of the rationality of definable integrals avoiding resolution of singularities but making use instead of a Cell-Decomposition Theorem which allows one to integrate I one variable at a time. The proof in [DvdD] of the rationality of integrals definable in L_{AN} depends on resolution of singularities but van den Dries gives in his paper [vdD] a proof without resolution of singularities. We omit the details but it is a straightforward corollary, as in Denef's paper [D2], to deduce the above theorem from van den Dries's proof. ∎

We show now how to parameterize the zeta functions $\zeta^*_{G,p}(s)$ for $G \in \mathcal{U}_{d,p}$ and $* \in \{\leq, \triangleleft\}$. In [duS2] we defined a language L_G for uniform pro-p groups containing function symbols for multiplication and p-adic exponentiation in G together with a binary relation defining the lower p-series in G, $\{G^{p^i}\}_{i\in\mathbf{N}}$. If $d\nu$ denotes the normalized Haar measure on G we showed in that same paper how to express $\zeta^*_{G,p}(s)$ as an integral

$$(*) \qquad \int_{N^*_{G,p}} p^{-h(g_1,\ldots,g_d)s-k(g_1,\ldots,g_d)}d\nu$$

where $h\colon G^{(d)} \to \mathbf{Z}$, $k\colon G^{(d)} \to \mathbf{Z}$ and $N^*_{G,p} \subseteq G^{(d)}$ are definable in L_G.

Fix a set of topological generators $x_1, \ldots, x_d$ for G. Then G can be identified with the set of all p-adic words of the form:

$$x_1^{a_1} \cdots x_d^{a_d}$$

with $\bar{a} = (a_1, \ldots, a_d) \in \mathbf{Z}_p^d$. This is a general property of uniform pro-p groups. Lazard called these "coordinates of the second kind". He proved (see [La1] or [DduSMS]) that there exist power series defining multiplication and exponentiation with respect to this coordinate system. In [duS2] we used these facts to write the L_G-definable integral $(*)$ as an integral definable in L_{AN}. Alternatively we could have used the "coordinates of the first kind", which are defined via the intrinsic Lie algebra $L(G)$ defined on G. Each element of G has a unique expression of the form

$$x(\bar{a}) = a_1x_1 + \cdots + a_dx_d$$

with $\bar{a} = (a_1, \ldots, a_d) \in \mathbf{Z}_p^d$. These are known as the coordinates of the first kind. In [La1] IV.3.4.4 and [DduSMS] Exercise 9.3 it is proved that these coordinates define the same manifold structure as the coordinates of the second kind. It follows then that there exist power series $F_{G,l}(\bar{X},\bar{Y}) \in \mathbf{Q}_p[[\bar{X},\bar{Y}]]$ $(l = 1,\dots,d)$ such that

$$x(\bar{a}).x(\bar{b}) = x\big(\bar{F}_G(\bar{a},\bar{b})\big).$$

Exponentiation is defined in a much more straightforward manner with respect to these coordinates:

$$x(\bar{a})^\lambda = x(\lambda\bar{a}).$$

In the same fashion as [duS2] we can use this coordinate system to replace the integral $(*)$ by an integral

$$\int_{M^*_{G,p}} | f(\bar{m}) |^s | g(\bar{m}) | \, d\mu$$

where $f, g\colon \mathbf{Q}_p^{d^2} \to \mathbf{Q}_p$ are L_{AN}-definable functions depending only on d and

$$M^*_{G,p} = \big\{\bar{m} = (m_{ij}) \in \mathrm{M}_d(\mathbf{Z}_p) \mid \Phi^*(\bar{m}) \text{ is true in } \mathbf{Q}_p\big\}$$

where $\Phi^*(X_{ij}; 1 \le i,j \le d)$ is an L_{AN}-formula defined using the analytic functions $F_{G,l}$ $(l = 1,\dots,d)$. In the same manner as for nilpotent groups, to parameterize these integrals for $G \in \mathcal{U}_{d,p}$ it will suffice to show that we can parameterize the functions $F_{G,l}$ $(l = 1,\dots,d)$ defining multiplication in uniform pro-p groups of dimension d with respect to coordinates of the first kind. To do this we use the fact that the group operation on G can be recovered from the intrinsic Lie algebra $L(G)$ via the Baker–Campbell–Hausdorff series. This will allow us to parameterize the functions $F_{G,l}$ using the structure constants of the Lie algebra $L(G)$.

Lemma 4.7: *There exist power series $F_l(\bar{X},\bar{Y},C_{ijk}; 1 \le i,j,k \le d)$, $l = 1,\dots,d$, such that if $G \in \mathcal{U}_{d,p}$ then the functions $F_{G,l}(\bar{X},\bar{Y})$ (defining multiplication in G with respect to a chosen basis $x_1,\dots,x_d$ of G) have the following form:*

$$F_{G,l}(\bar{X},\bar{Y}) = F_l(\bar{X},\bar{Y},a_{ijk}(G); 1 \le i,j,k \le d)$$

where $\big(a_{ij1}(G)\big),\dots,\big(a_{ijd}(G)\big) \in \mathbf{Z}_p^{d^3}$ are the structure constants of the intrinsic Lie algebra of G with respect to the chosen basis $x_1,\dots,x_d$, i.e. $(x_i,x_j) = \sum_{k=1}^d a_{ijk}(G)x_k$.

Proof: Let $\Phi(X,Y) = \sum_{n=1}^\infty u_n(X,Y)$ denote the Baker-Campbell-Hausdorff series where $u_n(X,Y) = \sum_{\bar{e}} q_{\bar{e}}(X,Y)_{\bar{e}}$ is a summation, over all vectors $\bar{e} =$

$(e_1, \ldots, e_s)$ of positive integers satisfying $< \bar{e} >= e_1 + \cdots + e_s = n-1$, of left-normed repeated Lie brackets

$$(X,Y)_{\bar{e}} = (X, \underbrace{Y, \ldots, Y}_{e_1}, \underbrace{X, \ldots, X}_{e_2}, \ldots).$$

Let $x, y \in G$ then

$$x.y = \Phi_{L(G)}(x,y) = \sum_{n=1}^{\infty} u_n(x,y)$$

where addition and the Lie bracket on G are taken to be the intrinsic Lie algebra operations defined on $L(G)$. (For details of this fact consult [DduSMS] Chapter 10 using the stronger estimate for the size of the coefficients $q_{\bar{e}}$ given by Lazard [La2], namely

$$q_{\bar{e}}.p^{(<\bar{e}>-1)/(p-1)} \in \mathbf{Z}_p;$$

alternatively IV.3.2.6 of [La1] and section 4 of [I] also contain details of this result.)

Let $\big(a_{ij1}(G)\big), \ldots, \big(a_{ijd}(G)\big) \in \mathbf{Z}_p^{d^3}$ be the structure constants of the intrinsic Lie algebra of G with respect to some choice of basis $x_1, \ldots, x_d$ so that

$$(x_i, x_j) = \sum_{k=1}^{d} a_{ijk}(G) x_k.$$

In a similar manner to Lemma 10.9 of [DduSMS], for each $\bar{e} = (e_1, \ldots, e_s)$, there exist polynomials $P^l_{\bar{e}}(\bar{X}, \bar{Y}, C_{ijk}; 1 \le i,j,k \le d)$, $l = 1, \ldots, d$, such that for each $G \in \mathcal{U}_{d,p}$

$$\big(x(\bar{a}), x(\bar{b})\big)_{\bar{e}} = \sum_{l=1}^{d} P^l_{\bar{e}}\big(\bar{a}, \bar{b}, a_{ijk}(G)\big) x_l$$

for all $\bar{a}, \bar{b} \in \mathbf{Z}_p^d$. Since

$$\begin{aligned} x\big(\bar{F}(\bar{a},\bar{b})\big) &= x(\bar{a}).x(\bar{b}) \\ &= \Phi_L\big(x(\bar{a}), x(\bar{b})\big) \\ &= \sum_{l=1}^{d} \Big(\sum_{\bar{e}} q_{\bar{e}} P^l_{\bar{e}}\big(\bar{a}, \bar{b}, a_{ijk}(G)\big) \Big) x_l \\ &= x\Big(\sum_{\bar{e}} q_{\bar{e}} P^1_{\bar{e}}\big(\bar{a}, \bar{b}, a_{ijk}(G)\big), \ldots, \sum_{\bar{e}} q_{\bar{e}} P^d_{\bar{e}}\big(\bar{a}, \bar{b}, a_{ijk}(G)\big) \Big) \end{aligned}$$

we can choose $F_l(\bar{X},\bar{Y},C_{ijk}(G);1 \leq i,j,k \leq d)$ to be the power series $\sum_{\bar{e}} q_{\bar{e}} P^l_{\bar{e}}(\bar{X},\bar{Y},C_{ijk})$. This completes the proof of Lemma 4.7. ∎

Hence, using the power series $F_l(\bar{X},\bar{Y},C_{ijk}(G);1 \leq i,j,k \leq d)$ in $\bar{X},\bar{Y}$ and C_{ijk}, $l = 1,\ldots,d$, we can define subsets $A^* \subseteq \mathbf{Z}_p^{d^2} \times \mathbf{Z}_p^{d^3}$ such that $M^*_{G,p} = A^*(a_{ijk}(G))$. So $\zeta^*_{G,p}(s) = I(f,g,A^*,a_{ijk}(G),s)$ for $* \in \{\leq,\triangleleft,\}$. We can therefore apply Theorem 4.6 and Proposition 4.5 (ii) to deduce

THEOREM 4.8: *Let $d \in \mathbf{N}$ and p prime. There exist $a_j,b_j \in \mathbf{Z}$ $(j = 1,\ldots,h)$ such that for $* \in \{\leq,\triangleleft,\wedge\}$ and $G \in \mathcal{U}_{d,p}$ there exists a polynomial $\Psi^*_{G,p} \in \mathbf{Q}[X]$ such that*

$$\zeta^*_{G,p}(s) = \frac{\Psi^*_{G,p}(p^{-s})}{\prod_{j\leq h}(1-p^{-a_js-b_j})}.$$

Combining this with Proposition 4.5 and Theorem 3.2 we also get uniformity in the prime p:

COROLLARY 4.9: *Let $d \in \mathbf{N}$. There exist $a_j,b_j \in \mathbf{Z}$ $(j = 1,\ldots,h)$ such that for each prime p, $* \in \{\leq,\triangleleft,\wedge\}$ and $G \in \mathcal{U}_{d,p}$ there exists a polynomial $\Psi^*_{G,p}(X) \in \mathbf{Q}_p[X]$ such that*

$$\zeta^*_{G,p}(s) = \frac{\Psi^*_{G,p}(p^{-s})}{\prod_{j\leq h}(1-p^{-a_js-b_j})}..$$

Note that the fact that one can recover G from its Lie algebra via the Baker–Campbell–Hausdorff series implies an equivalence of categories between d-dimensional uniform pro-p groups and d-dimensional powerful $\mathbf{Z}_p$-Lie algebras (see IV.3.2.6 of [La1]). Hence the parameter space we defined in section 3 for powerful d-dimensional $\mathbf{Z}_p$-Lie algebras is also a parameter space for the class of uniform pro-p groups of dimension d. We can prove similar results to the end of section 3 about the behaviour of the map $Z^*\colon \mathcal{U}_{d,p} \to \mathbf{Q}[[X]]$ defined by $G \longmapsto \zeta^*_{G,p}(s)$ on this parameter space.

Finally we consider how we can extend Theorem 4.8 to the class of compact p-adic analytic groups. Let G be a compact p-adic analytic group with a normal uniform subgroup G_0 of finite index in G. In [duS2] it is shown how to extend the integrals counting subgroups and normal subgroups in G_0 to integrals counting subgroups and normal subgroups in G. In this case we will lose the possibility of proving uniformity in p since these integrals are defined over the analytic language L_{AN} which has no uniformity properties at present and we can no longer hope to use the Lie algebra which only gives us information about subgroups in G_0.

However, if we fix the prime p, we can parameterize these integrals if we restrict ourselves to the class $\mathcal{G}_{n,d,p}$ of compact p-adic analytic groups G containing a d-dimensional normal uniform subgroup of index n. We have to bound the index n since these integrals are in $(d+n)d$ variables. Let $F_i(\bar{X},\bar{Y}) \in \mathbf{Q}_p[[\bar{X},\bar{Y}]]$ $(i=1,\ldots,d)$ denote the power series defining the group operation on the uniform subgroup G_0 as above. Let $y_1,\ldots,y_n$ be a transversal for G_0 in G. Then there exist power series $H_{ij}(\bar{X}) \in \mathbf{Q}_p[[\bar{X}]]\,(i=1,\ldots,d, j=1,\ldots,n)$ such that for each $j=1,\ldots,n$

$$y_j x(\bar{a}) y_j^{-1} = x(\bar{a})^{y_j} = x\big(\bar{H}_j(\bar{a})\big).$$

By [duS2], for $* \in \{\leq, \triangleleft\}$, there exist L_{AN}-definable functions $f, g\colon \mathbf{Q}_p^{(d+n)d} \to \mathbf{Q}_p$ and a subset

$$M^*_{G,p} = \big\{\bar{m} = (m_{ij}) \in \mathrm{M}_{(d+n)\times d}(\mathbf{Z}_p) \mid \Phi^*(\bar{m}) \text{ is true in } \mathbf{Q}_p\big\}$$

where $\Phi^*(X_{ij}; 1 \leq i \leq d+n, 1 \leq j \leq d)$ is an L_{AN}-formula defined now using the analytic functions F_i $(i=1,\ldots,d)$ and H_{ij} $(i=1,\ldots,d, j=1,\ldots,n)$, such that

$$\zeta^*_{G,p}(s) = \int_{M^*_{G,p}} |\, f(\bar{m})\,|^s |\, g(\bar{m})\,|\, d\mu.$$

The task now becomes to parameterize the functions $H_i(\bar{X})$ $i=1,\ldots,d$ defining the coordinates of an automorphism $\varphi\colon G_0 \to G_0$ such that

$$x(\bar{a})^{\varphi} = x\big(\bar{H}(\bar{a})\big).$$

But an automorphism of G induces a Lie algebra automorphism of the underlying Lie algebra $L(G)$ (see [DduSMS] Chapter 4). Therefore the power series $H_i(\bar{X})$, $i=1,\ldots,d$, with respect to the coordinates of the first kind are just given by multiplication by a matrix $D_\varphi = (d_{ij\varphi}) \in \mathrm{GL}_d(\mathbf{Z}_p)$, i.e.

$$x(\bar{a})^{\varphi} = x(\bar{a}D_\varphi).$$

Hence we can define subsets

$$A^* \subseteq \mathbf{Z}_p^{(d+n)d} \times \mathbf{Z}_p^{d^3} \times \mathbf{Z}_p^{nd^2}$$

using the power series $F_l(\bar{X},\bar{Y},C_{ijk}(G); 1 \leq i,j,k \leq d)$, $l=1,\ldots,d$, of Lemma 4.7 and the matrices $D_m = (D_{ijm})$, $m=1,\ldots,d$, such that

$$M^*_{G,p} = A^*\big(a_{ijk}(G), d_{ijm}\big)$$

where $(d_{ijm}) = D_{y_m}$. Applying Theorem 4.6 we can deduce:

THEOREM 4.10: *Let $d, n \in \mathbf{N}$ and p prime. There exist $a_j, b_j \in \mathbf{Z}$ $(j = 1, \ldots, h)$ such that for $* \in \{\leq, \lhd\}$ and $G \in \mathcal{G}_{n,d,p}$ there exists a polynomial $\Psi^*_{G,p} \in \mathbf{Q}[X]$ such that*

$$\zeta^*_{G,p}(s) = \frac{\Psi^*_{G,p}(p^{-s})}{\prod_{j \leq h}(1 - p^{-a_j s - b_j})}.$$

Since the technique for expressing $\zeta^{\wedge}_{G,p}(s)$ as a definable integral for a uniform group depends on using the Lie algebra associated with G it seems less clear how we can extend Theorem 4.8 to a uniformity result for $\zeta^{\wedge}_{G,p}(s)$ in the case that G is a compact p-adic analytic group.

References

[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] J. Denef, *On the evaluation of certain p-adic integrals*, Séminaire de Théorie des Nombres Paris 1983–84, Progress in Math. **59** (1985), 25–47.

[DvdD] J. Denef and L. van den Dries, *p-adic and real subanalytic sets*, Ann. of Math. **128** (1988), 79–138.

[DduSMS] J. D. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal, *Analytic pro-p groups*, L.M.S. Lecture Note Series 157, CUP, 1991.

[duS1] M.P.F. du Sautoy, *Finitely generated groups, p-adic analytic groups and Poincaré series*, Bull. Amer. Math. Soc. **23** (1990), 121–126.

[duS2] M.P.F. du Sautoy, *Finitely generated groups, p-adic analytic groups and Poincaré series*, Ann. of Math. **137** (1993), 639–670.

[duSL] M. P. F. du Sautoy and A. Lubotzky, *Functional equations and uniformity for local zeta functions of nilpotent groups*, in preparation.

[GS] F. J. Grunewald and D. Segal, *Reflections on the classification of torsion-free nilpotent groups*, in *Group Theory: Essays for Philip Hall* (K. W. Gruenberg and J. E. Roseblade, eds.), Academic Press, New York, 1984.

[GSS] F.J. Grunewald, D. Segal and G.C. Smith, *Subgroups of finite index in nilpotent groups*, Invent. Math. **93** (1988), 185–223.

[H] P. Hall, *Nilpotent groups*, Queen Mary College Math. Notes, 1969.

[I] I. Ilani, *Analytic pro-p groups and their Lie algebras*, to appear.

[La1] M. Lazard, *Groupes analytiques p-adiques*, Inst. Hautes Études Sci. Publ. Math. **26** (1965), 389–603.

[La2] M. Lazard, *Quelques calculs concernant la formule de Hausdorff*, Bull. Soc. Math. France **91** (1963), 435–451.

[M1] A. Macintyre, *On definable subsets of p-adic fields*, J. Symb. Logic **41** (1976), 605–610.

[M2] A. Macintyre, *Rationality of p-adic Poincaré series: uniformity in p*, Ann. Pure Appl. Logic **49** (1990), 31–74.

[P1] J. Pas, *Uniform p-adic cell decomposition and local zeta functions*, J. Reine Angew. Math. **399** (1989), 137–172.

[P2] J. Pas, *Cell decomposition and local zeta functions in a tower of unramified extensions of a p-adic field*, Proc. L.M.S. **60** (1990), 37–67.

[S] D. Segal, *Polycyclic Groups*, Cambridge University Press, Cambridge, 1983.

[vdD] L. van den Dries, *Analytic Ax–Kochen–Ersov Theorems*, in *Proceedings of the International Conference on Algebra*, Contemporary Math., Vol. 131, Part 3, American Mathematical Society, 1992, pp. 379–398.