PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

MARCUS DU SAUTOY

Counting p-groups and nilpotent groups

Publications mathématiques de l'I.H.É.S., tome 92 (2000), p. 63-112

<http://www.numdam.org/item?id=PMIHES_2000__92__63_0>

COUNTING p-GROUPS AND NILPOTENT GROUPS

by MARCUS DU SAUTOY

1. Introduction

Animals are divided into:

(a) belonging to the Emperor;
(b) embalmed;
(c) tame;
(d) sucking pigs;
(e) sirens;
(f) fabulous;
(g) stray dogs;
(h) included in the present classification;
(i) frenzied;
(j) innumerable;
(k) drawn with a very fine camel hair brush;
(l) et cetera;
(m) having just broken the water pitcher;
(n) that from a long way off look like flies.

Borges quoting from "A certain Chinese encyclopaedia".

Classification is perhaps one of the great themes of Mathematics, not least in group theory. In the 1890's the work of Killing and E. Cartan provided a classification of the simple Lie groups via their Dynkin diagrams. The 1980's saw the completion of the classification of finite simple groups. However, if we take even the least mysterious of the simple groups, the cyclic group of order a prime p, we still don't have a sensible classification of how we can put such groups together to build groups of order a power of p. In fact it has been considered that no such meaningful classification will materialize and we will just have to relegate p-groups to categories (i) and (j) of Borges *Chinese encyclopaedia.*

But there are attempts afoot to give some order to p-groups. In this paper we introduce zeta functions as a tool for studying finite groups which offers new insight into two existing approaches to the taming of p-groups. In Part I we apply zeta functions to an approach introduced by Graham Higman in the sixties. If you can't say what the groups of order p^n look like, you might attempt to at least say how many there are and rescue p-groups from the fate of Borges's classification (j). In Part II

we take a more recent structural approach introduced very successfully in the eighties by Charles Leedham-Green and Mike Newman. They suggested to sort p-groups with respect to a new invariant called the coclass of a p-group. A p-group of order p^n and nilpotency class c is said to have *coclass* $r = n - c$.

Part I concerns the following counting function and various refinements:

Definition **1.1.** — *Let p be a prime, n an integer and denote by*

$$f(n, p) = \textit{the number of } p\textit{-groups (up to isomorphism) of order } p^n.$$

The following table shows the majority of our current knowledge of the explicit values of $f(n, p)$ based on computer computation:

$f(1, p) = 1$
$f(2, p) = 2$
$f(3, p) = 5$
$f(4, 2) = 14$ $f(4, p) = 15$ for p odd
$f(5, 2) = 51$ $f(5, 3) = 67$ $f(5, p) = 2p + 2\gcd(p - 1, 3) + \gcd(p - 1, 4) + 61$ for $p \geqslant 5$
$f(6, p)$ is given by a quadratic polynomial in p whose coefficients depend on p mod 60.

Higman and Sims (see [22] and [38]) gave an asymptotic formula for the behaviour of this function as n grows (and p is fixed):

(**1**) $$f(n, p) = p^{(2/27 + o(1))n^3} \text{ as } n \to \infty.$$

However Higman predicted a more subtle behaviour of this function as you vary the prime p and fix n which starts to reveal itself in the above evidence for $n = 5$ and 6. This is encapsulated in what has become known as Higman's PORC conjecture:

Conjecture **1.2.** **(PORC)** — *For fixed n there is an integer* N *and polynomials* $\mathrm{P}_{n,i}(\mathrm{X})$ *for* $0 \leqslant i \leqslant \mathrm{N} - 1$ *so that if* $p \equiv i \bmod \mathrm{N}$ *then*

$$f(n, p) = \mathrm{P}_{n,i}(p).$$

PORC stands for Polynomial On Residue Classes. Higman's PORC conjecture has withstood any attack since Higman's own contribution in [23] in which he proved that counting class 2 elementary abelian p by elementary abelian p-groups was PORC.

In this paper we introduce a new tool, a zeta function, for tackling the enumeration of finite p-groups. This is defined as follows:

Definition **1.3.** — *Let p be a prime. For integers n, c, d define $\mathscr{P}(c, d, p)$ to be the set of finite p-groups (up to isomorphism) of class at most c generated by at most d generators and put*

$$f(n, p, c, d) = \operatorname{card}\left\{G \in \mathscr{P}(c, d, p) : |G| = p^n\right\}.$$

Define the zeta function of class c, d-generator p-groups to be:

$$\begin{aligned}\zeta_{c,d,p}(s) &= \sum_{n=0}^{\infty} f(n, p, c, d)p^{-ns} \\ &= \sum_{G \in \mathscr{P}(c,d,p)} |G|^{-s}.\end{aligned}$$

This is a generalization of a classical function introduced to count finite abelian groups which has a nice description in terms of the Riemann zeta function: let $\mathscr{A}(d)$ denote the finite abelian groups (up to isomorphism) of rank at most d then

$$\zeta_{\mathscr{A}(d)}(s) = \sum_{A \in \mathscr{A}(d)} |A|^{-s} = \zeta(s)\zeta(2s)\cdots\zeta(ds).$$

In fact there is an Euler product here expressing the fact that an abelian group is a direct product of abelian p-groups:

$$\zeta_{\mathscr{A}(d)}(s) = \prod_{p \text{ prime}} \zeta_{1,d,p}(s).$$

Since finite nilpotent groups are direct products of finite p-groups we can use the zeta functions counting p-groups to count nilpotent groups:

Definition **1.4.** — *For integers n, c, d define $\mathscr{N}(c, d)$ to be the set of finite nilpotent groups (up to isomorphism) of class at most c generated by at most d generators and put*

$$g(n, c, d) = \operatorname{card}\{G \in \mathscr{N}(c, d) : |G| = n\}.$$

Define the zeta function of class c, d-generator nilpotent groups to be:

$$\begin{aligned}\zeta_{c,d}(s) &= \sum_{n=1}^{\infty} g(n, c, d)n^{-s} \\ &= \sum_{G \in \mathscr{N}(c,d)} |G|^{-s}.\end{aligned}$$

In this paper we prove the following theorems which generalize the classical results for finite abelian groups:

Theorem **1.5.** — *For integers c and d there exists an Euler product*

$$\zeta_{c,d}(s) = \prod_{p \text{ prime}} \zeta_{c,d,p}(s).$$

Theorem **1.6.** — *For a fixed prime p and integers c and d, the function* $\zeta_{c,d,p}(s)$ *is a rational function in* p^{-s}.

Corollary **1.7.** — *For a fixed prime p and integers c and d the function* $f(n) = f(n, p, c, d)$ *satisfies a linear recurrence relation with constant coefficients.*

This Corollary shows the smooth behaviour when we fix a prime and count $f(n) = f(n, p, c, d)$ and offers some hope to rescue p-groups form Borges's classification (i).

As for fixing n and varying p, we have managed to put some algebraic geometry into the picture. Although this does not establish yet the strong uniformity predicted by Higman's PORC conjecture, we have established the following uniform behaviour:

Theorem **1.8.** — *For each c and d there exist finitely many subvarieties* $\mathrm{E}_{i,c,d}$ $(i \in \mathrm{T}(c, d))$ *of a variety* $\mathrm{Y}_{c,d}$ *defined over* $\mathbf{Q}$ *and for each* $\mathrm{I} \subset \mathrm{T}(c, d)$ *a rational function* $\mathrm{P}_{c,d,\mathrm{I}}(\mathrm{X}, \mathrm{Y}) \in \mathbf{Q}(\mathrm{X}, \mathrm{Y})$ *such that for almost all primes p*

$$\zeta_{c,d,p}(s) = \sum_{\mathrm{I} \subset \mathrm{T}(c,d)} e_{c,d,p,\mathrm{I}} \mathrm{P}_{c,d,\mathrm{I}}(p, p^{-s})$$

where

$$e_{c,d,p,\mathrm{I}} = \mathrm{card}\{a \in \overline{\mathrm{Y}_{c,d}}(\mathbf{F}_p) : a \in \overline{\mathrm{E}_{i,c,d}}(\mathbf{F}_p) \text{ if and only if } i \in \mathrm{I}\}.$$

Here $\overline{\mathrm{Y}}$ *means reduction of the variety* mod p *which is defined for almost all p.*

Since $f(n, p) = f(n, p, n-1, n)$ this Theorem for $\zeta_{n-1,n,p}(s)$ has the following corollary for the numbers $f(n, p)$:

Corollary **1.9.** — *For each n there exist finitely many subvarieties* $\mathrm{E}_{i,n}$ $(i \in \mathrm{T}(n))$ *of a variety* Y_n *defined over* $\mathbf{Q}$ *and for each* $\mathrm{I} \subset \mathrm{T}(n)$ *a polynomial* $\mathrm{H}_{n,\mathrm{I}}(\mathrm{X}) \in \mathbf{Q}[\mathrm{X}]$ *such that for almost all primes p*

$$f(n, p) = \sum_{\mathrm{I} \subset \mathrm{T}} e_{n,p,\mathrm{I}} \mathrm{H}_{n,\mathrm{I}}(p)$$

where

$$e_{n,p,\mathrm{I}} = \mathrm{card}\{a \in \overline{\mathrm{Y}_n}(\mathbf{F}_p) : a \in \overline{\mathrm{E}_{i,n}}(\mathbf{F}_p) \text{ if and only if } i \in \mathrm{I}\} .$$

So counting p-groups is given by the number of points on varieties mod p (or NOPOV, not quite as catchy as Higman's culinary shorthand). Not only that, the varieties $E_{i,c,d}$ are explicitly defined and arise from the resolution of singularities of a polynomial we associate to each pair (c, d). This theorem therefore offers some hope to approach Higman's PORC conjecture by analysing the nature of these varieties.

Using the analysis in [14] and [13] we can show that the uniform behaviour of the zeta functions in Theorem 1.8 implies the following asymptotic behaviour for the number $g(n, c, d)$ of nilpotent groups of order n, of class at most c, generated by at most d elements:

Theorem **1.10.** — *There exist a rational number* $\alpha(c, d) \in \mathbf{Q}$, *an integer* $\beta(c, d) \geqslant 0$ *and* $\gamma(c, d) \in \mathbf{R}$ *such that*

$$g(1, c, d) + \cdots + g(n, c, d) \sim \gamma(c, d) \cdot n^{\alpha(c,d)} (\log n)^{\beta(c,d)}.$$

This refines in some sense the result (1) of Higman and Sims.

The first part of the paper deals with counting p-groups of fixed class. To actually classify p-groups according to class looks rather hopeless as a list of such groups rapidly grows more and more complicated as c grows. The second part of the paper turns to a more fruitful invariant introduced in 1980 by Charles Leedham-Green and Mike Newman [28]. A p-group of order p^n and nilpotency class c is said to have *coclass* $r = n - c$. They made five Conjectures A to E, in decreasing order of strength, which offered some insight into how p-groups look when sorted with respect to this new invariant.

Remarkably these conjectures have now been confirmed. A proof of the strongest conjecture A can be found in Leedham-Green's paper [29] and Shalev's paper [37]. It says that although a p-group of fixed coclass will have class commensurate with the size of the p-group, nonetheless this p-group is close to being abelian.

Since the proof of these conjectures, a new set of conjectures due to Newman and O'Brien [32] has appeared on the scene, offering a more delicate description of a natural directed graph that can be built from p-groups of a given coclass. The vertices of this graph consist of all p-groups for a fixed prime p, one for each isomorphism type, and its edges are the pairs (P, Q) with P isomorphic to the quotient $Q/\gamma_c(Q)$ where $\gamma_c(Q)$ is the last non-trivial term of the lower central series of Q. One of the conjectures (Conjecture P) concerns the periodic behaviour of these graphs.

Each directed graph consists of a finite number of sporadic points together with a finite number of families $\mathscr{F}_G$ each consisting of a single infinite chain (whose inverse limit defines a pro-p group G) with finite twigs emanating from the points on the infinite chain. In the case of the prime $p = 2$, these twigs have bounded length. For each integer M, let $\mathscr{F}_G(M)$ denote the tree consisting of the infinite chain and twigs pruned to length at most M. Our main result of Part II is:

Theorem **1.11.** — *The tree* $\mathscr{T}_G(M)$ *is ultimately periodic.*

For $p=2$ this confirms the qualitative part of Conjecture P. Here "ultimately" means that there may be a finite piece at the top (the "tyranny of the small" as Newman refers to it) which needs to be chopped off before the tree becomes periodic.

The proof depends on proving the rationality of various associated zeta functions capturing the repetition of twigs of a particular shape, extending the spirit of the first part of the paper.

Let $c(r, n, p)$ denote the number of p-groups of order p^n and coclass r and define the Poincaré series of p-groups of coclass r to be

$$Z_{r,p}(X) = \sum_{n=0}^{\infty} c(r, n, p)X^n.$$

We prove the following theorem which provides some information about the unpruned trees $\mathscr{T}_G$:

Theorem **1.12.** — *For each* p *and* r, $Z_{r,p}(X)$ *is a rational function.*

All the proofs in this paper in some part depend on using another zeta function introduced to classify the unclassifiable by Grunewald, Segal and Smith [21]. The normal zeta function is defined for an infinite group G as follows:

$$\begin{aligned}\zeta_G^{\triangleleft}(s) &= \sum_{H \in \mathscr{N}(G)} |G : H|^{-s} \\ &= \sum_{n=1}^{\infty} a_n^{\triangleleft}(G)n^{-s}\end{aligned}$$

where $\mathscr{N}(G)$ denotes the set of normal subgroups of finite index in G. One can also define a zeta function counting all subgroups of finite index however it is this normal zeta function that will be relevant to us. Grunewald, Segal and Smith proposed these zeta functions as a tool in trying to understand the wild category of finitely generated nilpotent groups. These zeta functions of groups turn out to be functions with a lot of interesting properties. But they suffered a certain amount of criticism: although interesting in their own right, they did not serve as a very useful tool in the study of groups. The philosophy of this paper is that, although originally introduced for the study of infinite groups, zeta functions are a very powerful tool in understanding finite p-groups and nilpotent groups. I hope that this paper will answer some of these criticisms and stimulate group theorists to adopt these zeta functions as a potentially very powerful weapon in their arsenal.

The connection to the first part of the paper comes from the fact that the set of finite nilpotent groups $\mathscr{N}(c, d)$ is precisely the set of finite quotients up to isomorphism

of the free nilpotent group $F_{c,d}$ of class c on d generators. However the zeta function $\zeta^{\triangleleft}_{F_{c,d}}(s)$ is going to overcount these images since one finite nilpotent group can be realised as a finite quotient by several normal subgroups. But we can overcome this overcounting by introducing a correction factor into the zeta function $\zeta^{\triangleleft}_{F_{c,d}}(s)$. Define $\mathfrak{G}_p$ to be automorphism group of the pro-p completion $(\widehat{F_{c,d}})_p$ of $F_{c,d}$. Then we shall prove the following:

Theorem **1.13.**

$$\zeta_{c,d,p}(s) = \sum_{N \triangleleft (\widehat{F_{c,d}})_p} |(\widehat{F_{c,d}})_p : N|^{-s} |\mathfrak{G}_p : \mathrm{Stab}_{\mathfrak{G}_p}(N)|^{-1}.$$

With this theorem to hand we apply the machinery of definable p-adic integrals developed in [3], [4] and [8] and in particular the new concept of cone integrals introduced in [14] and [13].

We have focused so far on counting finite images of the free nilpotent group up to isomorphism. However as we shall explain, the results actually apply in a much broader context to counting finite images of any nilpotent or p-adic analytic group up to isomorphism.

This is particularly relevant in the applications in the second part of the paper to counting p-groups of fixed coclass and understanding the periodicity of the associated trees. The proof of Coclass Conjecture A allows us to define a sort of universal p-adic analytic pro-p group whose finite images capture all finite p-groups of coclass r. However it also has other images which are not of coclass r. Coclass at first sight looks very undefinable. But we prove that as a corollary of Conjecture A, we can capture coclass by definable sentences. This allows us to write down a definable integral which describes the zeta function $\zeta^{r,p}_{\mathrm{ccl}}(s) = Z_{r,p}(p^{-s})$ and by [8] and [4] prove Theorem 1.12.

We need to squeeze the model theory to its limit to prove the periodicity of Theorem 1.11. Counting numbers of groups doesn't say anything about the shape of the tree. However we can use the flexibility of the notion of definability to count the number of points in the tree which have certain descendant patterns: this is then enough to capture the notion of periodicity.

The last section contains a number of explicit examples of these rational functions counting coclass.

The results of this paper were announced in [9]. A gentler introduction to some of the themes exploited in the current paper can be found in [19].

Just as the last two centuries saw the classification of simple Lie groups and simple finite groups, both at first sight quite out of reach, maybe the dawn of the new century offers some hope to understand the class of finite p-groups and nilpotent groups. Who

knows, perhaps such a classification will be as exotic as Borges's menagerie of animals. We hope at least that the present paper offers some contribution to this project.

Acknowledgements. — I would like to thank the Royal Society for the support that their University Research Fellowship has provided me during the course of this piece of work. I would also like to thank Dan Segal whose support, advice and suggestions are always invaluable.

Notation.

$\mathscr{N}(F)$ denotes the set of normal subgroups of F of finite index.

$\mathscr{N}_p(F)$ denotes the set of normal subgroups of F of p-power index.

$\widetilde{\mathscr{N}}(F)$ denotes equivalence classes of $\mathscr{N}(F)$ under the action of the automorphism group of F.

$f(n, p)$ is the number of groups of order p^n.

$f(n, p, c, d)$ is the number of groups of order p^n of class bounded by c and generated by at most d elements.

$g(n, c, d)$ is the number of nilpotent groups of order n of class bounded by c and generated by at most d elements.

$c(r, n, p)$ is the number of groups of order p^n and coclass r.

Part I. Counting finite p-groups and nilpotent groups of class c

2. Euler products for the zeta functions counting finite nilpotent groups

We generalize the setting a little from the introduction.

Definition **2.1.** — *For any group* F *let* $\mathscr{G}(F)$ *(respectively* $\mathscr{G}_p(F)$, *p prime) denote the set of finite quotients (respectively finite p-quotients) of the group* F *up to isomorphism and set*

$$\zeta_{\mathscr{G}(F)}(s) = \sum_{G \in \mathscr{G}(F)} |G|^{-s}$$

$$\zeta_{\mathscr{G}_p(F)}(s) = \sum_{G \in \mathscr{G}_p(F)} |G|^{-s}.$$

If $F = F_{c,d}$ is the free nilpotent group of class c on d generators, then the set $\mathscr{G}(F)$ is all finite nilpotent groups of class less than or equal to c and with at most d generators, i.e. $\zeta_{\mathscr{G}(F_{c,d})}(s) = \zeta_{c,d}(s)$. Note that if $\widehat{F}$ denotes the profinite completion and $\widehat{F}_p$ denotes the pro-p completion of F then $\zeta_{\mathscr{G}(F)}(s) = \zeta_{\mathscr{G}(\widehat{F})}(s)$ and $\zeta_{\mathscr{G}_p(F)}(s) = \zeta_{\mathscr{G}(\widehat{F}_p)}(s)$ (see section 1 of [21]).

We are going to use the zeta function counting normal subgroups in F to understand the zeta function $\zeta_{\mathscr{G}(F)}(s)$. Recall that this is defined in [21] as follows:

Definition **2.2.** — *For any group* F *let* $\mathscr{X}(F)$ *(respectively* $\mathscr{X}_p(F)$*) denote the set of normal subgroups of finite index (respectively p-power index) in* F. *Then*

$$\zeta_F^{\triangleleft}(s) = \sum_{H \in \mathscr{X}(F)} |F : H|^{-s}$$

$$\zeta_{F,p}^{\triangleleft}(s) = \sum_{H \in \mathscr{X}_p(F)} |F : H|^{-s}.$$

Each normal subgroup of finite index gives rise to a finite group in the set $\mathscr{G}(F)$. However the zeta function counting normal subgroups overcounts the finite images of F since each finite image appears in several ways as a finite image of F. It is interesting to compare the expressions in the case of $F = \mathbf{Z}^d$, the rank d free abelian group. As we indicated in the introduction

$$\zeta_{\mathscr{G}(F)}(s) = \sum_{A \in \mathscr{A}(d)} |A|^{-s} = \zeta(s)\zeta(2s) \cdots \zeta(ds)$$

whilst

$$\zeta_F^{\triangleleft}(s) = \zeta(s)\zeta(s-1) \cdots \zeta(s-d+1)$$

(see [21]).

We introduce an equivalence relation on the set $\mathscr{X}(F)$ and count equivalence classes. Let Aut(F) denote the group of automorphisms of F.

Definition **2.3.** — *Call two subgroups* H_1 *and* $H_2 \in \mathscr{X}(F)$ *equivalent if there exists an automorphism* $g \in \mathrm{Aut}(F)$ *such that* $gH_1 = H_2$. *Let* $\widetilde{\mathscr{X}(F)}$ *denote the set of equivalence classes. Define the index* $|F : \tilde{N}|$ *of an equivalence class* $\tilde{N}$ *to be the index of any representative for the class in* F *and then define the zeta function:*

$$\zeta_{\widetilde{\mathscr{X}(F)}}(s) = \sum_{\tilde{N} \in \widetilde{\mathscr{X}(F)}} |F : \tilde{N}|^{-s}.$$

Similarly we define a local zeta function for each prime p:

$$\zeta_{\widetilde{\mathscr{X}_p(F)}}(s) = \sum_{\tilde{N} \in \widetilde{\mathscr{X}_p(F)}} |F : \tilde{N}|^{-s}.$$

Since index is preserved by an automorphism $\widetilde{\mathscr{X}_p(F)} \subset \widetilde{\mathscr{X}(F)}$.

Note that equivalent subgroups define isomorphic finite quotients. It is not true in general though that an isomorphism between finite quotients can be lifted to an automorphism of F.

It is true, however, for suitable relatively free profinite groups. The following definition is taken from Chapter 15 of [20]:

Definition **2.4.** — *A family $\mathscr{C}$ of finite groups is called* almost full *if the following hold:*

(1) *$\mathscr{C}$ contains nontrivial groups;*

(2) *if $G \in \mathscr{C}$ then all homomorphic images and subgroups of G belong to $\mathscr{C}$;*

(3) *if $G_1, G_2 \in \mathscr{C}$ then $G_1 \times G_2 \in \mathscr{C}$.*

An inverse limit of $\mathscr{C}$ groups is called a pro-$\mathscr{C}$ group.

So for example we can take $\mathscr{C}$ to be finite p-groups, abelian groups, nilpotent groups or solvable groups.

Proposition **2.5.** — *Let $\mathscr{C}$ be an almost full family of finite groups and let F be a free pro-$\mathscr{C}$ group. Let H_1 and H_2 be normal subgroups of finite index in F. If F/H_1 and F/H_2 are isomorphic then there exists an automorphism g of F such that $gH_1 = H_2$.*

For a proof we refer to Proposition 15.31 of [20].

Corollary **2.6.** — *Let $\mathscr{C}$ be an almost full family of finite groups and let F be a free pro-$\mathscr{C}$ group. Then*

$$\zeta_{\mathscr{G}(F)}(s) = \zeta_{\widetilde{\mathscr{X}(F)}}(s).$$

Let $F = \widehat{F_{c,d}}$ denote the profinite completion of the free class c, d-generator nilpotent group. Then F is the free d-generator pro-$\mathscr{C}$ group where $\mathscr{C}$ is the class of finite nilpotent groups of class at most c. The set $\mathscr{G}(F)$ of finite quotients is then just the set $\mathscr{N}(c,d)$ of finite nilpotent groups that we are seeking to count. Similarly, if $\widehat{F}_p$ denotes the pro-p completion of $F_{c,d}$ then we get the same conclusion with finite groups replaced by finite p-groups. So we have the following:

Corollary **2.7.** — *Let F denote the profinite completion of the free class c d-generator nilpotent group and F_p its pro-p completion (or the Sylow p-subgroup of F). Then*

$$\zeta_{c,d}(s) = \zeta_{\widetilde{\mathscr{X}(F)}}(s)$$
$$\zeta_{c,d,p}(s) = \zeta_{\widetilde{\mathscr{X}(F_p)}}(s) = \zeta_{\widetilde{\mathscr{X}_p(F)}}(s).$$

We prove now a more general Euler product than that stated in the Introduction (Theorem 1.5).

Theorem **2.8.** — *Let* F *be a finitely generated nilpotent group (abstract or profinite). Then*

$$\zeta_{\mathscr{G}(\mathrm{F})}(s) = \prod_{p \text{ prime}} \zeta_{\mathscr{G}_p(\mathrm{F})}(s).$$

Proof. — If $G = F/N$ is a finite image of F then $G = G_{p_1} \times \ldots \times G_{p_r} \cong F/N_{p_1} \times \ldots \times F/N_{p_r}$ where G_{p_i} is the Sylow p_i-subgroup of G. Conversely if F/N_{p_i} $(i = 1, \ldots, r)$ is a finite p_i-image then setting $N = \bigcap N_{p_i}$, we get that $F/N \cong F/N_{p_1} \times \ldots \times F/N_{p_r}$ is a finite image of F. Also $F/N \cong F/M$ if and only if the corresponding Sylow p_i-subgroups are isomorphic. This sets up a 1-1 correspondence between finite images (up to isomorphism) G of F of order $n = p_1^{a_1} \ldots p_r^{a_r}$ and r-tuples $\left(G_{p_1}, \ldots, G_{p_r}\right)$ of images (up to isomorphism) of F where G_{p_i} has order $p_i^{a_i}$. Hence we get our Euler product. □

Corollary **2.9.**

$$\zeta_{c,d}(s) = \prod_{p \text{ prime}} \zeta_{c,d,p}(s).$$

In the case of a free pro-$\mathscr{C}$ group F we have shown that the function $\zeta_{\mathscr{G}(\mathrm{F})}(s)$ and its local factors $\zeta_{\mathscr{G}_p(\mathrm{F})}(s)$ are the same as the function $\zeta_{\widetilde{\mathscr{X}(\mathrm{F})}}(s)$ and its local factors $\zeta_{\widetilde{\mathscr{X}_p(\mathrm{F})}}(s)$. Hence the Euler product holds for the zeta function $\zeta_{\widetilde{\mathscr{X}(\mathrm{F})}}(s)$. However even in the general case when $\widehat{\mathrm{F}}$ is the profinite completion of a finitely generated nilpotent group F and these functions are potentially different we can prove an Euler product for $\zeta_{\widetilde{\mathscr{X}(\widehat{\mathrm{F}})}}(s)$.

Theorem **2.10.** — *Let* F *be a finitely generated nilpotent group. Then*

$$\zeta_{\widetilde{\mathscr{X}(\widehat{\mathrm{F}})}}(s) = \prod_{p \text{ prime}} \zeta_{\widetilde{\mathscr{X}_p(\widehat{\mathrm{F}})}}(s) = \prod_{p \text{ prime}} \zeta_{\widetilde{\mathscr{X}(\widehat{\mathrm{F}}_p)}}(s).$$

Proof. — The Euler product for $\zeta_{\widehat{\mathrm{F}}}^{\triangleleft}(s)$ (see [21]) already gives us a 1-1 correspondence between the normal subgroups N of $\widehat{\mathrm{F}}$ of index $n = p_1^{a_1} \ldots p_r^{a_r}$ and r-tuples $\left(N_{p_1}, \ldots, N_{p_r}\right)$ of normal subgroups of $\widehat{\mathrm{F}}$ of index $p_i^{a_i}$. The normal subgroups of index $p_i^{a_i}$ are in turn in 1-1 correspondence with subgroups of index $p_i^{a_i}$ in $\widehat{\mathrm{F}}_p$.

If there exists $g \in \mathrm{Aut}(\widehat{\mathrm{F}})$ with $gN_1 = N_2$ then it follows that g will map the corresponding r-tuples of subgroups of p_i-power index in $\widehat{\mathrm{F}}$ to each other. This automorphism also determines an automorphism of $\widehat{\mathrm{F}}_p$ which insures the equivalence of the corresponding subgroups of $\widehat{\mathrm{F}}_p$.

It is the converse that needs a little more thought and depends on the fact that the automorphism group $\mathrm{Aut}(\widehat{\mathrm{F}})$ has a decomposition as a product over primes p: $\mathrm{Aut}(\widehat{\mathrm{F}}) \cong \prod_p \mathrm{Aut}(\widehat{\mathrm{F}}_p)$. This decomposition follows from the corresponding decomposition for the profinite nilpotent group: $\widehat{\mathrm{F}} \cong \prod_p \widehat{\mathrm{F}}_p$. Suppose we have two r-tuples of subgroups $\left(\mathrm{N}_{p_1}, \ldots, \mathrm{N}_{p_r}\right)$ and $\left(\mathrm{M}_{p_1}, \ldots, \mathrm{M}_{p_r}\right)$ where $\mathrm{N}_{p_i}, \mathrm{M}_{p_i} \leqslant \widehat{\mathrm{F}}_{p_i}$ and there are automorphisms $g_i \in \mathrm{Aut}(\widehat{\mathrm{F}}_{p_i})$ with $g\mathrm{N}_{p_i} = \mathrm{M}_{p_i}$. Then the isomorphism $\mathrm{Aut}(\widehat{\mathrm{F}}) \cong \prod_p \mathrm{Aut}(\widehat{\mathrm{F}}_p)$ determines an automorphism $g \in \mathrm{Aut}(\widehat{\mathrm{F}})$ which ensures that the corresponding subgroups N and M in $\widehat{\mathrm{F}}$ satisfy $g\mathrm{N} = \mathrm{M}$. This gives us our Euler product. □

In the case that F is a finitely generated, torsion-free nilpotent group then Aut(F) has the structure of a $\mathbf{Q}$-algebraic subgroup $\mathfrak{G}$ of GL_n. We can describe this as follows (see Chapter 6 of [36]):

F has a natural embedding into the unipotent group of upper triangular matrices $\mathrm{Tr}_n^1(\mathbf{Z})$. Then the automorphism group of the Mal'cev completion (or radicable hull) $\mathrm{F}^{\mathbf{Q}}$ of F is isomorphic to the automorphism group of the $\mathbf{Q}$-Lie algebra $\mathscr{L}_{\mathrm{F}}(\mathbf{Q}) = \mathbf{Q}\log \mathrm{F}$, which has the structure of a $\mathbf{Q}$-algebraic subgroup $\mathfrak{G}(\mathbf{Q})$ of $\mathrm{GL}_n(\mathbf{Q})$. For example, if $\mathrm{F} = \mathbf{Z}^d$, the free abelian group, then $\mathfrak{G}(\mathbf{Q}) = \mathrm{GL}_d(\mathbf{Q})$ and $\mathrm{Aut}(\mathrm{F}) = \mathfrak{G}(\mathbf{Z}) = \mathrm{GL}_d(\mathbf{Z})$. Recall that by [2] we can realise any $\mathbf{Q}$-algebraic group with any given representation as the automorphism group of a nilpotent group modulo its IA-automorphisms. (IA-automorphisms are those which act trivially modulo the commutator subgroup.) In general Aut(F) will not necessarily be the $\mathbf{Z}$-points of $\mathfrak{G}$. We need to make an extra assumption on F.

The group F is called *a lattice group* if $\log \mathrm{F}$ is an additive subgroup. In this case we can choose a basis for this lattice $\log \mathrm{F}$ and identify the automorphism group Aut(F) of F with $\mathfrak{G}(\mathbf{Z})$. Also if $\mathrm{R} \geqslant \mathbf{Z}$ is any binomial ring (for which F^{R} is then defined) we can identify $\mathrm{Aut}(\mathrm{F}^{\mathrm{R}}) = \mathfrak{G}(\mathrm{R})$. In general Aut(F) is an arithmetic subgroup of $\mathfrak{G}(\mathbf{Q})$, i.e. commensurable with $\mathfrak{G}(\mathbf{Z})$ with respect to some choice of basis for $\mathscr{L}_{\mathrm{F}}(\mathbf{Q})$.

Note that if F is a lattice group then $\mathrm{Aut}(\widehat{\mathrm{F}}) = \mathfrak{G}(\widehat{\mathbf{Z}}) = \prod_p \mathfrak{G}(\mathbf{Z}_p)$ where $\mathrm{Aut}(\widehat{\mathrm{F}}_p) = \mathfrak{G}(\mathbf{Z}_p)$. Even if F is not lattice group then for almost all primes p, $\mathrm{Aut}(\widehat{\mathrm{F}}_p) = \mathfrak{G}(\mathbf{Z}_p)$.

In Theorem 2.10, we proved the existence of an Euler product for the zeta function counting finite images up to isomorphism of the profinite completion of F. Does an abstract finitely generated nilpotent group have such an Euler product without going to the profinite completion? This seems to depend on the class number of the algebraic automorphism group being 1. A similar issue arose in [21] where the zeta function counting subgroups of a nilpotent group G which were isomorphic to G failed to have an Euler product, whilst if you count those subgroups whose profinite completions are isomorphic to the profinite completion of G then you do get an Euler product.

We already have a one-to-one correspondence between subgroups N of finite index in F and subgroups (N_p) of finite index in $\prod_{p \text{ prime}} \widehat{F}_p$. We can define the *genus* of N with respect to $\mathrm{Aut}(\widehat{F})$ to be the set of subgroups corresponding to the orbit of (N_p) under the action of $\mathrm{Aut}(\widehat{F}) \cong \prod_p \mathrm{Aut}(\widehat{F}_p)$. The *class* of N is the orbit under the action of Aut(F). We then define

$$f_{\mathrm{Aut}(F)}(N) = \text{ number of classes in the genus of N.}$$

Then $f_{\mathrm{Aut}(F)}(N)$ is equal to the number of double cosets $\mathrm{Aut}(F)g\ \mathrm{Stab}_{\mathrm{Aut}(\widehat{F})}((N_p))$ in $\mathrm{Aut}(\widehat{F})$. The Euler product

$$\zeta_{\widetilde{\mathscr{K}(F)}}(s) = \prod_{p \text{ prime}} \zeta_{\widetilde{\mathscr{K}(\widehat{F}_p)}}(s)$$

is equivalent then to $f_{\mathrm{Aut}(F)}(N) = 1$ for all N. Note that $f_{\mathrm{Aut}(F)}(N)$ is finite for all N since the number of cosets of $\mathrm{Stab}_{\mathrm{Aut}(\widehat{F})}((N_p))$ in $\mathrm{Aut}(\widehat{F})$ is bounded by the number of subgroups of index $|F : N|$ in F.

If F is a lattice group and its automorphism group $\mathfrak{G}$ has strong approximation then we can prove such an Euler product. The group $\mathfrak{G}$ is said to have *(absolute) strong approximation* if the diagonal embedding $\mathfrak{G}(\mathbf{Q}) \hookrightarrow \prod_{p \text{ prime}} \mathfrak{G}(\mathbf{Z}_p) \times \mathfrak{G}(\mathbf{R}) = \mathfrak{G}(A(\infty))$ is dense where $A(\infty)$ is the ring of integral adeles. This is equivalent to the solvability of a certain system of congruences. In particular it says that for $a = \left(a_{p_1}, \ldots, a_{p_r}\right) \in \mathfrak{G}(\mathbf{Z}_{p_1}) \times \ldots \times \mathfrak{G}(\mathbf{Z}_{p_r})$ and $n \in \mathbf{N}$ there exists $x \in \mathfrak{G}(\mathbf{Q})$ with the property that $x \equiv a_{p_i} \bmod p_i^n$ for $i = 1, \ldots, r$. Strong approximation is an algebraic geometric version of the Chinese Remainder Theorem. Hence for N and aN in the same genus we can take n large enough (since N and aN are open subgroups in G) so that xN $= a$N, i.e. N and aN are in the same class and $f_{\mathfrak{G}(\mathbf{Z})}(N) = 1$ for all N. We therefore have

Theorem **2.11.** — *If* F *is a lattice group and* $\mathfrak{G}$ *has strong approximation then*

$$\zeta_{\widetilde{\mathscr{K}(F)}}(s) = \prod_{p \text{ prime}} \zeta_{\widetilde{\mathscr{K}(\widehat{F}_p)}}(s).$$

A **Q**-algebraic group has strong approximation if and only if its reductive part H is simply connected and does not contain any simple component H^i with $H^i(\mathbf{R})$ compact. A proof of this was first provided by Platonov in [33] and [34]. For details on strong approximation and the subtle properties of class numbers of algebraic groups we refer the reader to [35].

3. Rationality of the zeta function counting p-groups

The Euler products of the previous section are something special about nilpotent groups. In this section we move away from the special setting of nilpotent groups and consider images arising from a general p-adic analytic pro-p group.

Let G be a p-adic analytic pro-p group and $\mathfrak{G}$ is its automorphism group. In this section we prove the following:

Theorem **3.1.** — $\zeta_{\widetilde{\mathscr{K}(G)}}(s)$ *is a rational function in* p^{-s}.

Recall that in [8] we proved that the zeta function

$$\zeta_G^{\triangleleft}(s) = \sum_{H \in \mathscr{K}(G)} |G : H|^{-s}$$

is a rational function in p^{-s}. The size of the orbit of H under the action of $\mathfrak{G}$ is equal to the index of the stabilizer of H in $\mathfrak{G}$. Hence we have the following:

Lemma **3.2.**

$$\zeta_{\widetilde{\mathscr{K}(G)}}(s) = \sum_{H \in \mathscr{K}(G)} |G : H|^{-s} |\mathfrak{G} : \mathrm{Stab}_{\mathfrak{G}}(H)|^{-1}.$$

This is similar to a zeta function that we considered in [8] where we counted conjugacy classes of subgroups of G. We can use a similar approach to there to prove the rationality of this zeta function. In section 1 of [8] we introduced the language $\mathscr{L}_G$ and proved the rationality of definable integrals over p-adic analytic pro-p groups G. The proof depends on translating these $\mathscr{L}_G$-definable integrals into definable integrals in the analytic language $\mathscr{L}_{\mathrm{an}}^D$ introduced by Denef and van den Dries [4] by exploiting the p-adic coordinate system of G. We therefore aim to represent our zeta function as an $\mathscr{L}_G$-definable integral.

The key to being able to do this is the concept of a good basis for subgroups in a uniform p-adic analytic pro-p group G_1. We recall this definition (Definition 2.2 of [8]). The lower p-series G_n of G_1 is defined as $G_n = G_{n-1}^p [G_{n-1}, G_1]$ for $n > 1$ (for a reference on uniform groups and the lower p-series see [7]). Let $u_1, \ldots, u_d$ be a minimal generating set for G_1. Then every element x of G_1 can be uniquely represented as a product of p-adic powers of this generating set: there exists a unique d-tuple $(\lambda_1, \ldots, \lambda_d) \in \mathbf{Z}_p^d$ such that

$$x = u_1^{\lambda_1} \ldots u_d^{\lambda_d} = \mathbf{u}(\lambda).$$

Define $\omega(x) = n$ if $x \in G_n \backslash G_{n+1}$. Note that $\mathbf{u}(\lambda) \in G_n$ if and only if $\lambda \in p^{n-1}\mathbf{Z}_p^d$.

The first order language $\mathscr{L}_{G_1}$ is defined as follows. As well as the usual logical symbols (including equality), the language has two sorts: those of sort x to be interpreted as elements of the uniform pro-p group G_1 and those of sort λ to be interpreted as p-adic integers. It has function symbols $x \cdot y$, x^{-1}, x^{λ}, $\phi_\alpha(x)$ to be interpreted respectively as the product, inverse, λth power and certain automorphisms of G_1 (to be specified). There are constant symbols of the first sort representing fixed elements of G_1. Finally, there is a binary relation symbol $x|y$ to be interpreted as $\omega(x) \geqslant \omega(y)$.

The definition of a good basis for a subgroup H_1 generalizes the concept and properties of the minimal generating set of the uniform group G_1 :

Definition **3.3.** — *Let* H_1 *be an open subgroup of* G_1. *Then a d-tuple* $(h_1, ..., h_d)$ *of elements of* H_1 *is a* good basis *for* H_1 *if*

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

(ii) *for each* $n \leqslant m$, *the set*

$$\left\{ h_i^{p^{n-\omega(h_i)}} G_{n+1} \mid i = 1, ..., d;\ \omega(h_i) \leqslant n \right\}$$

is a basis for the $\mathbf{F}_p$*-vector space* $(H \cap G_n)G_{n+1}/G_{n+1}$.

Note that a good basis for G_1 is a minimal generating set. Subgroups H_1 may be generated by fewer than d elements but certainly H_1 can be generated by d elements, i.e. G_1 has rank d. A good basis for a subgroup H_1 has the same property as a minimal generating set for G_1, namely every element of H_1 can be represented uniquely as $h_1^{\lambda_1} ... h_d^{\lambda_d} = \mathbf{h}(\lambda)$ where $\lambda_i \in \mathbf{Z}_p$.

The compact p-adic analytic pro-p group G contains an open uniform characteristic pro-p group G_1. For each subgroup K with $G_1 \leqslant K \leqslant G$, define $\mathscr{H}(G, K) = \{H \in \mathscr{H}(G) : G_1 H = K\}$. For each such subgroup K we choose a right transversal $(y_1, ..., y_m)$ for G_1 in G with the property that $(y_1, ..., y_n)$ is a right transversal for G_1 in K. It suffices to prove that

$$\begin{aligned} \zeta_{\mathscr{H}(G,K)}(s) &= \sum_{H \in \mathscr{H}(G,K)} |G : H|^{-s} |\mathfrak{G} : \mathrm{Stab}_{\mathfrak{G}}(H)|^{-1} \\ &= |G : K|^{-s} \sum_{H \in \mathscr{H}(G,K)} |K : H|^{-s} |\mathfrak{G} : \mathrm{Stab}_{\mathfrak{G}}(H)|^{-1} \end{aligned}$$

is a rational function in p^{-s}.

Definition **3.4.** — (1) *Let* $H \in \mathscr{H}(G, K)$. *We call an n-tuple* $(t_1, ..., t_n)$ *of elements of* G_1 *a transversal basis for* H *if* $(t_1 y_1, ..., t_n y_n)$ *is a right transversal for* $H_1 = H \cap G_1$ *in* H.

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

(3) *For a subgroup* $H \in \mathscr{X}(G, K)$ *define a subset* $M(H)$ *of* $G_1^{(d+n)} = G_1 \times \ldots \times G_1$ *by* $M(H) = \{(h_1, \ldots, h_d, t_1, \ldots, t_n)$ is a basis for $H\}$.

Let μ denote the Haar measure on $G_1^{(d+n)}$. In [8] an integral was defined over $M(H)$ expressing $|K : H|^{-s}$. Put

$$r_k = \text{card}\{j : \omega(h_j) = k\}$$
$$s_k = r_1 + \cdots + r_k$$
$$s_0 = 0$$

where $(h_1, \ldots, h_d)$ is a good basis for $H_1 = H \cap G_1$. The integrand in [8] is actually incorrect and we take this opportunity to give the correct version. The error occurred due to an incorrect calculation of the measure of the set $GL_{r_k}(\mathbf{Z}_p)$ which should be $(1 - p^{-1})(1 - p^{-2})\ldots(1 - p^{-r_k}) = \phi(r_k)$, say, rather than $(1 - p^{-1})^{r_k}$. Then the measure of $M(H)$ is given by

$$\mu(M(H)) = \phi(h_1, \ldots, h_d) \prod_{i=1}^{d} p^{2i+n-1} p^{-(i+n)\omega(h_i) - \omega(h_{i+1}) - \cdots - \omega(h_d)}$$

where $\phi(h_1, \ldots, h_d) = \phi(r_1)\ldots\phi(r_k)$ and $\omega(h_{s_i+1}) = \ldots = \omega(h_{s_{i+1}}) < \omega(h_{s_{i+1}+1})$. Define functions $h : G_1^{(d+n)} \to \mathbf{N}$ and $k : G_1^{(d+n)} \to \mathbf{N}$ and c by

$$h(\mathbf{g}) = \omega(g_1) + \cdots + \omega(g_d)$$
$$k(\mathbf{g}) = \sum_{i=1}^{d} (2i + n - 1)\omega(g_i)$$
$$c = \prod_{i=1}^{d} p^{s-2i-n+1} = p^{ds - d^2 - dn}.$$

Then since $|K : H|^{-s} = |G_1 : H \cap G_1|^{-s} = p^{(d-h(\mathbf{g}))s}$ for any choice of basis $(g_1, \ldots, g_{d+n})$ for H we have that

$$|K : H|^{-s} = c \int_{M(H)} \phi(g_1, \ldots, g_d) p^{-sh(\mathbf{g})+k(\mathbf{g})} d\mu$$
$$= c \int_{M(H)} F(\mathbf{g}) d\mu.$$

Note that $\phi(g_1, \ldots, g_d)$ is still a definable function since we can definably partition $G^{(d)}$ into a finite number of subsets on which the function is constant so its introduction has not affected the definability of the integral representing $|K : H|^{-s}$.

We now pull out our trump card in this setting. The automorphism group $\mathfrak{G}$ of the p-adic analytic group G is itself a p-adic analytic group (see Theorem 5.7 of

[7]). Hence we can apply the same analysis as above to understand the subgroups of $\mathfrak{G}$. Let $\mathfrak{G}_1$ be an open uniform normal subgroup of $\mathfrak{G}$ of dimension r. (We won't need to insist that it be characteristic as we have done for G_1. We shall see soon why we need this assumption for G_1.) For each subgroup $\mathfrak{K}$ with $\mathfrak{G}_1 \leqslant \mathfrak{K} \leqslant \mathfrak{G}$, define $\mathscr{H}(G, K, \mathfrak{K}) = \{H \in \mathscr{H}(G) : G_1H = K \text{ and } \mathrm{Stab}_{\mathfrak{G}}(H)\mathfrak{G}_1 = \mathfrak{K}\}$. For each choice of such a subgroup $\mathfrak{K}$ choose a right transversal $(v_1, ..., v_s)$ for $\mathfrak{G}_1$ in $\mathfrak{G}$ with the property that $(v_1, ..., v_t)$ is a right transversal for $\mathfrak{G}_1$ in $\mathfrak{K}$. It suffices to prove that

$$\zeta_{\mathscr{H}(G,K,\mathfrak{K})}(s) = \sum_{H \in \mathscr{H}(G,K,\mathfrak{K})} |G : H|^{-s} |\mathfrak{G} : \mathrm{Stab}_{\mathfrak{G}}(H)|^{-1}$$
$$= |G : K|^{-s} |\mathfrak{G} : \mathfrak{K}|^{-1} \sum_{H \in \mathscr{H}(G,K,\mathfrak{K})} |K : H|^{-s} |\mathfrak{K} : \mathrm{Stab}_{\mathfrak{G}}(H)|^{-1}$$

is a rational function in p^{-s}.

For each $H \in \mathscr{H}(G, K, \mathfrak{K})$ define

$$N(H) = \left\{ (u_1, ..., u_r, s_1, ..., s_t) \in \mathfrak{G}_1^{(r+t)} : (\mathbf{u}, \mathbf{s}) \text{ is a basis for } \mathrm{Stab}_{\mathfrak{G}}(H) \right\}.$$

Let ν denote the Haar measure on $\mathfrak{G}_1^{(r+t)}$. Then

$$|\mathfrak{K} : \mathrm{Stab}_{\mathfrak{G}}(H)|^{-1} = c' \int_{N(H)} \phi(x_1, ..., x_r) p^{-h'(\mathbf{x})+k'(\mathbf{x})} d\nu$$
$$= c' \int_{N(H)} F'(\mathbf{x}) d\nu$$

where h', k', c' and F' are the functions h, k, c and F with d and n replaced by r and t respectively.

Let

$$\mathscr{M} = \bigcup_{H \in \mathscr{H}(G,K,\mathfrak{K})} M(H) \times N(H) \subset G_1^{(d+n)} \times \mathfrak{G}_1^{(r+t)}.$$

Then

$$\sum_{H \in \mathscr{H}(G,K,\mathfrak{K})} |K : H|^{-s} |\mathfrak{K} : \mathrm{Stab}_{\mathfrak{G}}(H)|^{-1} \tag{2}$$
$$= cc' \int_{\mathscr{M}} F(\mathbf{g}) F'(\mathbf{x}) d\mu d\nu.$$

Since the integrand has already been shown to be definable in [8], our task is to prove that the subset $\mathscr{M}$ is a definable subset of $G_1^{(d+n)} \times \mathfrak{G}_1^{(r+t)}$ in the sense of Definition 1.14 of [8]. Although we have two uniform subgroups on the go, we can think of this as a definable subset in $(d+n+r+t)$ copies of the pro-p group $G_1 \times \mathfrak{G}_1$ constructed as a semi-direct product with $\mathfrak{G}_1$ acting on the characteristic subgroup G_1 by automorphisms. By a suitable choice of $\mathfrak{G}_1$ we can actually assume that $G_1 \times \mathfrak{G}_1$ is a uniform group,

namely choose $\mathfrak{G}_1$ to be contained in the kernel of the natural map $\mathfrak{G} \to \mathrm{Aut}(G_1/G_1^p)$. Note that G_1 and $\mathfrak{G}_1$ are definable subgroups in $G_1 \times \mathfrak{G}_1$ since, for example, any element of G_1 is expressible as a product of p-adic powers of a basis chosen for G_1.

To prove that $\mathscr{M}$ is definable in $\mathscr{L}_{G_1 \times \mathfrak{G}_1}$ it will suffice to prove that the following statements are definable:

(1) $(h_1, ..., h_d, t_1, ..., t_n)$ is a basis for some normal subgroup H of G with $HG_1 = K$;

(2) $(u_1, ..., u_r, s_1, ..., s_t)$ is a basis for some subgroup $\mathfrak{H}$ of $\mathfrak{G}$ with $\mathfrak{H}\mathfrak{G}_1 = \mathfrak{K}$;

(3) $\mathfrak{H} = \mathrm{Stab}_{\mathfrak{G}}(H)$.

The first two are definable as established in Lemma 2.12 and Theorem 2.15 of [8].

To prove that (3) is definable we follow a similar argument to that outlined in section 2.3.3 of [8] where the normalizer of a subgroup is shown to be definable. Since $u_1, ..., u_r$ and $s_1 v_1, ..., s_t v_t$ generate the subgroup $\mathfrak{H}$ topologically, $\mathfrak{H} = \mathrm{Stab}_{\mathfrak{G}}(H)$ if and only if

(a) $u_1, ..., u_r$ and $s_1 v_1, ..., s_t v_t$ stabilize H;

(b) if $1 \leqslant i \leqslant s$ and $x \in \mathfrak{G}_1$, and xv_i stabilizes H then there exists $\mu \in \mathbf{Z}_p^r$ and $1 \leqslant j \leqslant t$ such that

$$xv_i = u_1^{\mu_1} \ldots u_r^{\mu_r} s_j v_j.$$

Therefore to prove that (a) and (b) are definable it suffices to prove the statement "xv_i stabilizes H" is definable. Since $(h_1, ..., h_d, t_1, ..., t_n)$ is a basis for H, every element of H has a unique expression of the form $h_1^{\lambda_1} \ldots h_d^{\lambda_d} t_j y_j$. So xv_i stabilizes H is equivalent to the conjunction of statements for $j = 1, ..., n$ of

$$\bigvee_{k=1}^{n} \forall \lambda \in \mathbf{Z}_p^d \exists \mu \in \mathbf{Z}_p^d \left(\left(h_1^{\lambda_1}, ..., h_d^{\lambda_d} t_j y_j \right)^{xv_i} = h_1^{\mu_1} \ldots h_d^{\mu_d} t_k y_k \right).$$

This is then a definable statement in the uniform group $G_1 \times \mathfrak{G}_1$ where we have symbols in the language $\mathscr{L}_{G_1 \times \mathfrak{G}_1}$ representing the action of the transversal elements $y_1, ..., y_m$ and $v_1, ..., v_s$ on the uniform group $G_1 \times \mathfrak{G}_1$.

So $\mathscr{M}$ is definable in $\mathscr{L}_{G_1 \times \mathfrak{G}_1}$ and hence by Theorem 1.17 of [8] the integral in (2) is a rational function in p^{-s}. Hence $\zeta_{\widetilde{\mathscr{X}(G)}}(s)$ is a rational function in p^{-s} and we have proved Theorem 3.1.

4. A simplification for nilpotent groups

Although theoretically powerful the definable integrals of the previous section are a little daunting to analyse. In this section we show how for a nilpotent group F, we can give a much more tractable integral expression for $\zeta_{\widetilde{\mathscr{X}(\hat{F}_p)}}(s)$ for almost all primes p. This expression allows some approach then to Higman's PORC conjecture as we shall explain.

The idea is to linearise the problem by considering the associated Lie algebra. As we have explained a finitely generated torsion-free nilpotent group F has a natural Lie algebra $\mathscr{L}_F(\mathbf{Q})$ over $\mathbf{Q}$ associated to it. Make a choice of a Lie subring L of $\mathscr{L}_F(\mathbf{Q})$ which is a full $\mathbf{Z}$-lattice in $\mathscr{L}_F(\mathbf{Q})$. The automorphism group of the Mal'cev completion (or radicable hull) $F^{\mathbf{Q}}$ of F is isomorphic to the automorphism group $\mathfrak{G}$ of the $\mathbf{Q}$-Lie algebra $\mathscr{L}_F(\mathbf{Q})$. $\mathfrak{G}$ is a $\mathbf{Q}$-algebraic group. A $\mathbf{Z}$-basis for L determines a representation for $\mathfrak{G}$ with the property that for almost all p, $\mathfrak{G}(\mathbf{Z}_p)$ is isomorphic to the automorphism group of $\hat{F}_p$.

For each prime p, define $\mathscr{X}(L_p)$ to be the set of ideals of finite index in $L_p = L \otimes \mathbf{Z}_p$. Define an equivalence relation on $\mathscr{X}(L_p)$ where two ideals N_1 and N_2 are equivalent if there exists $\varphi \in \mathfrak{G}(\mathbf{Z}_p) = \mathrm{Aut}(L_p)$ such that $N_1 = \varphi N_2$. Let $\widetilde{\mathscr{X}(L_p)}$ denote the set of equivalence classes and define

$$\zeta_{\widetilde{\mathscr{X}(L_p)}}(s) = \sum_{\tilde{N} \in \widetilde{\mathscr{X}(L_p)}} |L_p : \tilde{N}|^{-s}.$$

Then we have the following:

Lemma **4.1.** — *For almost all primes p*

$$\zeta_{\widetilde{\mathscr{X}(\hat{F}_p)}}(s) = \zeta_{\widetilde{\mathscr{X}(L_p)}}(s).$$

Proof. — For almost all primes p, $\log \hat{F}_p = L_p$ and $N \to \log N$ sets up a one-to-one index preserving correspondence between $\mathscr{X}(\hat{F}_p)$ and $\mathscr{X}(L_p)$. This follows from the analysis of section 4 of [21]. Since the isomorphism between the automorphism group of $\hat{F}_p$ and $\mathfrak{G}(\mathbf{Z}_p) = \mathrm{Aut}(L_p)$ is given by $\varphi \mapsto \log \circ \varphi \circ \exp$, the one-to-one correspondence between $\mathscr{X}(\hat{F}_p)$ and $\mathscr{X}(L_p)$ preserves the respective equivalence relations on these sets. Hence we get the equality of zeta functions claimed by the Lemma. □

Our first reduction is as before, namely:

$$\sum_{\tilde{N} \in \widetilde{\mathscr{X}(L_p)}} |L_p : \tilde{N}|^{-s} = \sum_{N \in \mathscr{X}(L_p)} |L_p : N|^{-s} |\mathfrak{G}(\mathbf{Z}_p) : \mathrm{Stab}_{\mathfrak{G}(\mathbf{Z}_p)}(N)|^{-1}.$$

The choice of basis for L allows one to identify L with $\mathbf{Z}^n$ and L_p with $\mathbf{Z}_p^n$. Let $\mathrm{Tr}_n(\mathbf{Z}_p)$ denote the set of upper triangular matrices. For each $N \in \mathscr{X}(L_p)$, define a subset $M(N) \subset \mathrm{Tr}_n(\mathbf{Z}_p)$ such that $M(N)$ consists of all matrices M whose rows $\mathbf{m}_1, \ldots, \mathbf{m}_n$ form a basis for N. Note that if $M \in M(N)$ then $N = \mathbf{Z}_p^n \cdot M = \left\{\lambda M : \lambda \in \mathbf{Z}_p^n\right\}$. Let μ denote the additive Haar measure on $\mathrm{Tr}_n(\mathbf{Z}_p)$. Then

$$|L_p : N|^{-s} = (1 - p^{-1})^{-n} \int_{M(N)} |m_{11}|^{s-1} \ldots |m_{nn}|^{s-n} d\mu.$$

(For a reference see section 3 of [21] with the warning that we prefer to use upper triangular matrices for basis rather than the lower triangular matrices of [21].)

Now $\mathfrak{G}(\mathbf{Z}_p)$ is then a subgroup of $\mathrm{GL}_n(\mathbf{Z}_p)$. We get a nice description of $\mathrm{Stab}_{\mathfrak{G}(\mathbf{Z}_p)}(N)$ in terms of $M \in M(N)$, namely:

$$\mathrm{Stab}_{\mathfrak{G}(\mathbf{Z}_p)}(N) = \mathfrak{G}(\mathbf{Z}_p) \cap M^{-1}\mathrm{GL}_n(\mathbf{Z}_p)M.$$

Let ν be the normalized Haar measure on $\mathfrak{G}(\mathbf{Z}_p)$. The value of $|\mathfrak{G}(\mathbf{Z}_p) : \mathrm{Stab}_{\mathfrak{G}(\mathbf{Z}_p)}(N)|^{-1}$ is then just the measure of the set $\mathfrak{G}(\mathbf{Z}_p) \cap M^{-1}\mathrm{GL}_n(\mathbf{Z}_p)M$. Hence

$$\begin{aligned} &|L_p : N|^{-s} |\mathfrak{G}(\mathbf{Z}_p) : \mathrm{Stab}_{\mathfrak{G}(\mathbf{Z}_p)}(N)|^{-1} \\ &\quad = (1 - p^{-1})^{-n} \int_{M(N)} |m_{11}|^{s-1} \ldots |m_{nn}|^{s-n} \nu\left(\mathfrak{G}(\mathbf{Z}_p) \cap M^{-1}\mathrm{GL}_n(\mathbf{Z}_p)M\right) d\mu. \end{aligned}$$

Define the subset $\mathscr{M} \subset \mathrm{Tr}_n(\mathbf{Z}_p) \times \mathfrak{G}(\mathbf{Z}_p)$ by

$$\mathscr{M} = \left\{(M, K) : M \in \bigcup_{N \in \mathscr{X}(L_p)} M(N),\ K \in \mathfrak{G}(\mathbf{Z}_p) \cap M^{-1}\mathrm{GL}_n(\mathbf{Z}_p)M\right\}$$

then

$$\zeta_{\widetilde{\mathscr{X}(L_p)}}(s) = (1 - p^{-1})^{-n} \int_{\mathscr{M}} |m_{11}|^{s-1} \ldots |m_{nn}|^{s-n} d\mu d\nu.$$

In section 3 of [21] it is shown that the condition $M \in \bigcup_{N \in \mathscr{X}(L_p)} M(N) = V_p$, say, is expressible as a definable formula in the language of valued fields $\mathscr{L}_{\mathrm{al}}$ independent of p. We recall the condition since it is quite straightforward. Let $\beta : \mathbf{Z}^n \times \mathbf{Z}^n \to \mathbf{Z}^n$ be the bilinear map expressing the Lie bracket in L with respect to the chosen basis. Then a matrix $M \in V_p$ if and only if

$$\text{for } 1 \leqslant i, j \leqslant n \exists Y_{ij}^1, \ldots, Y_{ij}^n \in \mathbf{Z}_p$$

$$\text{such that } \beta(\mathbf{m}_i, \mathbf{e}_j) = \sum_{k=1}^{n} Y_{ij}^k \mathbf{m}_k.$$

This condition checks whether the additive lattice generated by elements whose coordinates are the rows of M actually is an ideal in L_p. In section 5 of [14] we showed that by solving these equations we can represent this condition by a simple sort of condition called a *cone condition.*

Definition **4.2.** — *Call a formula* $\psi(\mathbf{x})$ *in the first order language for the valued field* $\mathbf{Q}_p$ *a cone condition over* $\mathbf{Q}$ *if there exist polynomials* $f_i(\mathbf{x}), g_i(\mathbf{x})\,(i=1,...,l)$ *over* $\mathbf{Q}$ *in the variables* $\mathbf{x}=x_1,...,x_m$ *such that* $\psi(\mathbf{x})$ *is a conjunction of formulas*

$$v(f_i(\mathbf{x})) \leqslant v(g_i(\mathbf{x}))$$

for $i=1,...,l$.

It is instructive to know how the polynomials in the cone condition for V_p are defined as they are explicitly constructible from the structure constants defining L and very amenable to direct analysis. We therefore reproduce the details contained in [14].

We can express the defining conditions for V_p in matrix form which makes things quite transparent. Let C_j denote the matrix whose rows are $\mathbf{c}_i=\beta(\mathbf{e}_i, \mathbf{e}_j)$.

$M \in V_p$ if we can solve for each $1 \leqslant i,j \leqslant n$ the equation

$$\mathbf{m}_i C_j = \left(Y_{ij}^1, ..., Y_{ij}^n\right) M$$

with $\left(Y_{ij}^1, ..., Y_{ij}^n\right) \in \mathbf{Z}_p^n$. Let M′ denote the adjoint matrix and

$$M^\natural = M' \mathrm{diag}(m_{22}^{-1} ... m_{nn}^{-1} \; ... \; m_{nn}^{-1}, \; 1).$$

Then since the matrix M is upper triangular, the ikth entry of $M^\natural$ is a homogeneous polynomial of degree $k-1$ in the variables m_{rs} with $1 \leqslant r \leqslant s \leqslant k-1$. Then we can rewrite the above equation as:

$$\mathbf{m}_i C_j M^\natural = \left(m_{11} Y_{ij}^1, ..., m_{11} ... m_{nn} Y_{ij}^n\right).$$

Let $g_{ijk}(m_{rs})$ denote the kth entry of the n-tuple $\mathbf{m}_i C_j M^\natural$ which is a homogeneous polynomial of degree k in m_{rs}. (In fact we can see that it is homogeneous of degree 1 in m_{is} $(s=1,...,n)$ and degree $k-1$ in m_{rs} with $1 \leqslant r \leqslant s \leqslant k-1$.)

Then

$$V_p = \left\{(m_{rs}) \in \mathrm{Tr}_n(\mathbf{Z}_p) : v(m_{11}, ..., m_{kk}) \leqslant v(g_{ijk}(m_{rs})) \text{ for } i,j,k \in \{1,...,n\}\right\}.$$

We collect together the simplifications of this section in the following:

Theorem **4.3.** — *Let* F *be a finitely generated, torsion-free nilpotent group. Let* L *be a choice of a* $\mathbf{Z}$*-Lie algebra spanning the natural Lie algebra* $\mathscr{L}_F(\mathbf{Q})$ *over* $\mathbf{Q}$ *associated to* F. *Let* $\mathfrak{G}$

denote the $\mathbf{Q}$*-algebraic automorphism group of* $\mathscr{L}_F(\mathbf{Q})$ *with underlying* $\mathbf{Z}$*-structure defined such that* $\mathfrak{G}(\mathbf{Z}) = \mathrm{Aut}(L)$. *Put* $L_p = L \otimes \mathbf{Z}_p$.

(1) *For almost all primes* p,

$$\zeta_{\widetilde{\mathscr{X}(\widehat{F}_p)}}(s) = \zeta_{\widetilde{\mathscr{X}(L_p)}}(s).$$

(2) *There exist polynomials* $g_{ijk}(m_{rs})$ *for* $i, j, k \in \{1, \ldots, n\}$ *such that for all primes* p,

$$\zeta_{\widetilde{\mathscr{X}(L_p)}}(s) = (1 - p^{-1})^{-n} \int_{\mathscr{M}} |m_{11}|^{s-1} \ldots |m_{nn}|^{s-n} d\mu dv$$

where the subset $\mathscr{M} \subset \mathrm{Tr}_n(\mathbf{Z}_p) \times \mathfrak{G}(\mathbf{Z}_p)$ *is defined by*

$$\mathscr{M} = \left\{ \begin{array}{c} ((m_{rs}), K) : v(m_{11}, \ldots, m_{kk}) \leqslant v(g_{ijk}(m_{rs})) \text{ for } i, j, k \in \{1, \ldots, n\}, \\ K \in \mathfrak{G}(\mathbf{Z}_p) \cap M^{-1}\mathrm{GL}_n(\mathbf{Z}_p)M \end{array} \right\}$$

and $d\mu$ *is the additive normalized Haar measure on* $\mathrm{Tr}_n(\mathbf{Z}_p)$ *and* dv *is the normalized Haar measure on* $\mathfrak{G}(\mathbf{Z}_p)$.

This formula is a bit more inviting to analyse. In particular to understand how these functions vary with the prime p will depend on understanding two pieces:

(1) one coming from the zeta function counting ideals in L or normal subgroups in the free nilpotent group; and

(2) the other coming from the algebraic group $\mathfrak{G}$ and the behaviour of the measure $\mathfrak{G}(\mathbf{Z}_p) \cap M^{-1}\mathrm{GL}_n(\mathbf{Z}_p)M$.

Note that the second statement of Theorem 4.3 holds also for a Lie ring L additively isomorphic to $\mathbf{Z}^n$ even if it is not nilpotent.

In the next sections we return to the special case described in the Introduction where F is a free nilpotent group.

5. PORC and counting points on varieties mod p

We move away from the general setting of the last few sections where we counted finite p-groups as images of an arbitrary nilpotent or p-adic analytic group. Instead we return to trying to understand the numbers

$$f(n, p) = \text{the number of } p\text{-groups (up to isomorphism) of order } p^n$$

and for $c, d \in \mathbf{N}$ the more refined version of this counting function $f(n, p, c, d)$ defined as the number of groups (up to isomorphism) of order p^n, of class at most c, generated by at most d generators.

In this case we can apply the previous analysis to the case that $F = F_{c,d}$, the free d-generator nilpotent group of class c. Then

$$\zeta_{c,d,p}(s) = \zeta_{\mathscr{G}_p(F)}(s) = \zeta_{\widetilde{\mathscr{L}(\widehat{F_p})}}(s).$$

We begin by proving the following uniformity result for the behaviour of these functions as we vary p :

Theorem **5.1.** — *For each c and d, there exist finitely many subvarieties $E_{i,c,d}$ $(i \in T(c,d))$ of a variety $Y_{c,d}$ defined over $\mathbf{Q}$ and for each $I \subset T(c,d)$ a rational function $P_{c,d,I}(X, Y) \in \mathbf{Q}(X, Y)$ such that for almost all primes p*

$$\zeta_{c,d,p}(s) = \sum_{I \subset T(c,d)} e_{c,d,p,I} P_{c,d,I}(p, p^{-s})$$

where

$$e_{c,d,p,I} = \mathrm{card}\{a \in \overline{Y_{c,d}}(\mathbf{F}_p) : a \in \overline{E_{i,c,d}}(\mathbf{F}_p) \text{ if and only if } i \in I\}.$$

Here $\overline{Y}$ means reduction of the variety mod *p which is defined for almost all p.*

Since $f(n,p) = f(n,p,n-1,n)$ this Theorem for $\zeta_{n-1,n,p}(s)$ has the following corollary for the numbers $f(n,p)$:

Corollary **5.2.** — *For each n there exist finitely many subvarieties $E_{i,n}$ $(i \in T(n))$ of a variety Y_n defined over $\mathbf{Q}$ and for each $I \subset T(n)$ a polynomial $H_{n,I}(X) \in \mathbf{Q}(X)$ such that for almost all primes p*

$$f(n,p) = \sum_{I \subset T} e_{n,p,I} H_{n,I}(p)$$

where

$$e_{n,p,I} = \mathrm{card}\{a \in \overline{Y_n}(\mathbf{F}_p) : a \in \overline{E_{i,n}}(\mathbf{F}_p) \text{ if and only if } i \in I\} .$$

The proof relies on proving that the integrals of the previous section for free nilpotent groups are represented by *cone integrals*. We defined in the previous section the concept of a cone condition in the first order language for valued fields.

Definition **5.3.** — *Given a cone condition $\psi(\mathbf{x})$ over $\mathbf{Q}$ defined by polynomials $f_i(\mathbf{x})$, $g_i(\mathbf{x})$ $(i = 1, \ldots, l)$ and polynomials $f_0(\mathbf{x})$ and $g_0(\mathbf{x})$ with coefficients in $\mathbf{Q}$, we call an integral*

$$Z_{\mathscr{D}}(s,p) = \int_{V_p = \{\mathbf{x} \in \mathbf{Z}_p^m : \psi(\mathbf{x}) \text{ is valid}\}} |f_0(\mathbf{x})|^s \, |g_0(\mathbf{x})| \, |dx|$$

a cone integral defined over $\mathbf{Q}$, *where* $|dx|$ *is the normalized additive Haar measure on* $\mathbf{Z}_p^m$ *and* $\mathscr{D} = \{f_0, g_0, f_1, g_1, \ldots, f_l, g_l\}$ *is called the set of cone integral data.*

In [14] the following uniformity result was established for such integrals:

Theorem **5.4.** — *Let* (Y, h) *be a resolution over* $\mathbf{Q}$ *for* $f(\mathbf{x}) = \prod_{i=0}^{l} f_i(\mathbf{x})g_i(\mathbf{x})$ *and let* E_i, $i \in T$, *be the irreducible components defined over* $\mathbf{Q}$ *of the reduced scheme* $(h^{-1}(D))_{\text{red}}$ *where* $D = \text{Spec}\left(\frac{\mathbf{Q}[\mathbf{x}]}{(F)}\right)$. *Then for each* $I \subset T$ *there exists a rational function* $P_I(X, Y) \in \mathbf{Q}(X, Y)$ *with the property that for almost all primes* p

$$Z_{\mathscr{D}}(s, p) = \sum_{I \subset T} c_{p,I} P_I(p, p^{-s}) \tag{3}$$

where

$$c_{p,I} = \text{card}\{a \in \overline{Y}(\mathbf{F}_p) : a \in \overline{E_i} \text{ if and only if } i \in I\}$$

and $\overline{Y}$ *means the reduction mod* p *of the scheme* Y.

So by Theorem 4.3 to prove Theorem 5.1 it suffices to show that

$$(1 - p^{-1})^n \zeta_{\widetilde{\mathscr{X}(L_p)}}(s + n) = \int_{\mathscr{M}} |m_{11}|^{s+n-1} \ldots |m_{nn}|^s d\mu d\nu$$

is a cone integral where the subset $\mathscr{M} \subset \text{Tr}_n(\mathbf{Z}_p) \times \mathfrak{G}(\mathbf{Z}_p)$ is defined by

$$\mathscr{M} = \left\{ \begin{array}{c} ((m_{rs}), K) : v(m_{11}, \ldots, m_{kk}) \leqslant v(g_{ijk}(m_{rs})) \text{ for } i, j, k \in \{1, \ldots, n\}, \\ K \in \mathfrak{G}(\mathbf{Z}_p) \cap M^{-1}GL_n(\mathbf{Z}_p)M \end{array} \right\}.$$

We have already done part of the work since the condition defining when a matrix (m_{rs}) defines a basis for an ideal inside L_p is expressed by a cone condition. The task now is

(1) to rewrite the Haar measure $d\nu$ on $\mathfrak{G}(\mathbf{Z}_p)$ in terms of an additive Haar measure on $\mathbf{Z}_p^N$; and

(2) to prove that the condition $K \in \mathfrak{G}(\mathbf{Z}_p) \cap M^{-1}GL_n(\mathbf{Z}_p)M$ is given by a cone condition on K and M.

We begin with a description of the automorphism group $\mathfrak{G}$ of the free class c, d-generator nilpotent Lie algebra $\mathscr{L}(F)$ associated to F which will make everything transparent.

Let $u_1, \ldots, u_d$ be free generators for $\mathscr{L} = \mathscr{L}(F)$. Let $\gamma_i(\mathscr{L})$ denote the ith term of the lower central series of $\mathscr{L}$ and define $r_i = \dim_{\mathbf{Q}} \gamma_i(\mathscr{L})/\gamma_{i+1}(\mathscr{L})$ and $s_i = \dim_{\mathbf{Q}} \mathscr{L}/\gamma_{i+1}(\mathscr{L})$.

There are formulas given by Witt for these dimensions:

$$r_i = 1/i \sum_{j|i} \mu(j) d^{i/j}$$

where $\mu(j)$ is the Möbius function (see for example Theorem 5.11 of [30]). There exists a sequence of elements $z_1, ..., z_{s_c}$ called a *Witt basis* for $\mathscr{L}$ with the property that

(i) for $s_i + 1 \leqslant l \leqslant s_{i+1}$, $z_l = (u_{j_1(l)}, ..., u_{j_{i+1}(l)})$ (where $j_1(l), ..., j_{i+1}(l) \in \{1, ..., d\}$) is a homogeneous Lie commutator of length $i+1$ in the free generators $u_1, ..., u_d$; and

(ii) $z_{s_i+1}, ..., z_{s_c}$ form a linear basis over $\mathbf{Z}$ for the Lie elements of length $\geqslant i+1$.

See for example section 5.6 of [30].

Recall that the Lie algebra L is a choice of a $\mathbf{Z}$-lattice inside $\mathscr{L}$ which then determines a representation of the automorphism group $\mathfrak{G}$ and hence an associated $\mathbf{Z}$-structure on the algebraic group. We choose the lattice L to be the $\mathbf{Z}$-span of the basis $\{z_1, ..., z_{s_c}\}$ and define L_{i+1} to be the $\mathbf{Z}$-span of $\{z_{s_i+1}, ..., z_{s_{i+1}}\}$. We then have a decomposition

$$L = L_1 \oplus \cdots \oplus L_c.$$

This basis defines a $\mathbf{Q}$-rational representation $\rho : \mathfrak{G} \to GL_{s_c}$ with the property that $\mathrm{Aut}(L_p) = \mathfrak{G}(\mathbf{Z}_p) \leqslant GL_{s_c}(\mathbf{Z}_p)$. We consider each $\mathbf{Q}_p$-linear transformation α of the underlying vector space $\mathscr{L} \otimes \mathbf{Q}_p$ as represented by a $c \times c$ block matrix (α_{ij}) with $\alpha_{ij} \in \mathrm{Hom}_{\mathbf{Q}_p}(L_i \otimes \mathbf{Q}_p, L_j \otimes \mathbf{Q}_p)$. The following Proposition gives a description of $\mathfrak{G}(\mathbf{Z}_p)$ as a subset of $GL_{s_c}(\mathbf{Z}_p)$.

Proposition **5.5.** — *$\mathfrak{G}(\mathbf{Z}_p)$ consists of all $\mathbf{Q}_p$-linear transformations $\alpha = (\alpha_{ij})$ of the underlying vector space $\mathscr{L} \otimes \mathbf{Q}_p$ satisfying*

$$\alpha_{11} \in GL_d(\mathbf{Z}_p)$$
$$\alpha_{1j} \in M_{d, r_j}(\mathbf{Z}_p) \text{ for } 2 \leqslant j \leqslant c$$
$$\alpha_{ij} = \psi_{ij}(\alpha_{11}, ..., \alpha_{1, j-i+1}) \text{ for } 2 \leqslant i \leqslant j \leqslant c$$

where $\psi_{ij} = (\psi_{ijkl})$ is a matrix of $\mathbf{Q}$-polynomial maps ψ_{ijkl} depending only on $\mathscr{L}$ and independent of p.

For details see [17] and the references therein. Put $\psi_{1j}(\alpha_{11}, ..., \alpha_{1,j}) = \alpha_{1j}$.

We can now give a description of the Haar measure on $\mathfrak{G}(\mathbf{Z}_p)$. We identify $\mathfrak{G}(\mathbf{Z}_p)$ with $GL_d(\mathbf{Z}_p) \times \prod_{2 \leqslant j \leqslant c} M_{d, r_j}(\mathbf{Z}_p) \subset M_{d, s_c}(\mathbf{Z}_p)$.

Proposition **5.6.** — *Let $d\sigma$ denote the normalized additive Haar measure on $M_{d, s_c}(\mathbf{Z}_p)$. Let $c_p = \sigma(\mathfrak{G}(\mathbf{Z}_p)) = (1-p^{-1})(1-p^{-2})...(1-p^{-d})$. Then $c_p^{-1} \cdot d\sigma$ defines the normalized Haar measure on $\mathfrak{G}(\mathbf{Z}_p)$.*

For details combine Example 2 and Example 4 of Section 3.5 of [35]. (Note that because we are integrating on compact subgroups which are unimodular, we do not expect any gauge form in translating the additive Haar measure to a measure on $\mathfrak{G}(\mathbf{Z}_p)$. To define a Haar measure on $\mathfrak{G}(\mathbf{Q}_p)$ we would need to take $c_p^{-1}(\det \alpha_{11})^{-d} \cdot d\sigma$.)

Let M′ denote the adjoint matrix of M and

$$M^\natural = M' \mathrm{diag}(m_{22}^{-1} \ldots m_{nn}^{-1} \ldots m_{nn}^{-1}, 1).$$

The condition $K \in \mathfrak{G}(\mathbf{Z}_p) \cap M^{-1}GL_n(\mathbf{Z}_p)M$ now translates with respect to the coordinate system $\mathfrak{G}(\mathbf{Z}_p) \subset M_{d,s_c}(\mathbf{Z}_p)$ into the following condition: $(\mathbf{k}_{11}, \ldots, \mathbf{k}_{1c}) \in M_{d,s_c}(\mathbf{Z}_p)$ and $M \in \mathrm{Tr}_n(\mathbf{Z}_p)$ such that

(a) $\mathbf{k}_{11} \in GL_d(\mathbf{Z}_p)$ and $m_{11} \ldots m_{nn} \neq 0$; and

(b) there exists $\Lambda \in M_n(\mathbf{Z}_p)$ such that

$$M\left(\psi_{ij}\left(\mathbf{k}_{11}, \ldots, \mathbf{k}_{1,j-i+1}\right)\right) M^\natural = \Lambda \mathrm{diag}(m_{11}, \ldots, m_{11} \ldots m_{nn}). \tag{4}$$

Let $h_{kl}(M, \mathbf{k}_{11}, \ldots, \mathbf{k}_{1c})$ be the polynomial in the entries of $\mathbf{k}_{11}, \ldots, \mathbf{k}_{1c}$ and M defining the klth entry of $M\left(\psi_{ij}\left(\mathbf{k}_{11}, \ldots, \mathbf{k}_{1,j-i+1}\right)\right) M^\natural$. Then condition (4) becomes the following set of cone conditions:

(b)′ $(\mathbf{k}_{11}, \ldots, \mathbf{k}_{1c}) \in M_{d,s_c}(\mathbf{Z}_p)$ and $M \in \mathrm{Tr}_n(\mathbf{Z}_p)$ such that

$$v\left(h_{kl}(M, \mathbf{k}_{11}, \ldots, \mathbf{k}_{1c})\right) \geqslant v(m_{11} \ldots m_{ll}).$$

Note that in our integral we forget about condition (a) since the sets $\det \mathbf{k}_{11} = 0$ and $m_{11} \ldots m_{nn} = 0$ have measure 0. Hence we have proved the following expression for $\zeta_{\widetilde{\mathscr{B}(L_p)}}(s)$ in terms of a cone integral:

Theorem **5.7.**

$$c_p(1 - p^{-1})^n \zeta_{\widetilde{\mathscr{B}(L_p)}}(s + n) = \int_{\mathscr{N}} |m_{11}|^{s+n-1} \ldots |m_{nn}|^s d\mu d\sigma$$

is a cone integral where the subset $\mathscr{N} \subset \mathrm{Tr}_n(\mathbf{Z}_p) \times M_{d,s_c}(\mathbf{Z}_p)$ *is defined by*

$$\mathscr{N} = \left\{ \begin{array}{c} ((m_{rs}), \mathbf{k}_{11}, \ldots, \mathbf{k}_{1c}) : v(m_{11} \ldots m_{kk}) \leqslant v(g_{ijk}(m_{rs})) \text{ for } i, j, k \in \{1, \ldots, n\}, \\ \text{and } v(m_{11} \ldots m_{ll}) \leqslant v\left(h_{kl}(M, \mathbf{k}_{11}, \ldots, \mathbf{k}_{1c})\right) \text{ for } 1 \leqslant k, l \leqslant n \end{array} \right\}$$

and $d\mu \times d\sigma$ *is the additive Haar measure on* $\mathrm{Tr}_n(\mathbf{Z}_p) \times M_{d,s_c}(\mathbf{Z}_p)$.

This Theorem together with Theorem 5.4 proves Theorem 5.1. The statement of Theorem 5.4 and the analysis of this section mean that we can identify explicitly the varieties in Theorem 5.1. Since this will be very relevant in trying to understand PORC we take some time to record the definition of these varieties:

Definition **5.8.** — *Let $\mathscr{L}$ be the free class c, d-generator $\mathbf{Q}$-Lie algebra and let $z_1, \ldots, z_n$ be a Witt basis. Let $C_j = (c(j)_{kl})$ denote the $n \times n$ matrix with the property that $(z_k, z_j) = \sum_{l=1}^{n} c(j)_{kl} z_l$. Define the polynomial $F_{\mathscr{L}}(M, \mathbf{k}_{11}, \ldots, \mathbf{k}_{1c})$ with coefficients from $\mathbf{Q}$ in the entries $(M, \mathbf{k}_{11}, \ldots, \mathbf{k}_{1c}) \in \mathrm{Tr}_n(\mathbf{Q}) \times \mathrm{M}_{d, r_1}(\mathbf{Q}) \times \ldots \times \mathrm{M}_{d, r_c}(\mathbf{Q}) = \mathrm{Tr}_n(\mathbf{Q}) \times \mathrm{M}_{d, n}(\mathbf{Q})$ as a product of the following polynomials:*

(i) *polynomials $g_{ijk}(m_{rs})$ for $i, j, k \in \{1, \ldots, n\}$ defining the entries of $MC_jM^{\natural}$ for $j = 1, \ldots, n$;*

(ii) *polynomials $h_{kl}(M, \mathbf{k}_{11}, \ldots, \mathbf{k}_{1c})$ for $1 \leqslant k, l \leqslant n$ defining the klth entry of $M(\psi_{ij}(\mathbf{k}_{11}, \ldots, \mathbf{k}_{1, j-i+1}))M^{\natural}$ where ψ_{ij} are the polynomials in Proposition 5.5; and*

(iii) $m_{11}^{(n^2+n+1)n} \ldots m_{ii}^{(n^2+n+1)(n-i+1)} \ldots m_{nn}^{(n^2+n+1)}$.

Let $(Y_{c, d}, h)$ be a resolution over $\mathbf{Q}$ for $F_{\mathscr{L}}(M, \mathbf{k}_{11}, \ldots, \mathbf{k}_{1c})$ and define $E_{i, c, d}$, $i \in T(c, d)$, to be the irreducible components defined over $\mathbf{Q}$ of the reduced scheme $(h^{-1}(D))_{\mathrm{red}}$ where

$$D = \mathrm{Spec}\left(\frac{\mathbf{Q}[\mathbf{x}]}{(F_{\mathscr{L}})}\right).$$

It is then the varieties $E_i(c, d)$, $i \in T(c, d)$, which appear in the statement of Theorem 5.1. As we pointed out in Corollary 5.2 the case that $c = n - 1$ and $d = n$ is particularly relevant for Higman's PORC conjecture. We therefore make the following:

Definition **5.9.** — *For each n define $T(n) = T(n - 1, n)$ and $E_{i, n} = E_{i, n-1, n}$ for $i \in T(n)$.*

Then these are the varieties which appear in the corollary to Theorem 5.1.

Let us say a few words about how canonical the definition of the varieties $E_i(c, d)$ are. There are of course different ways to achieve the resolution of singularities of the polynomial $F_{\mathscr{L}}(M, \mathbf{k}_{11}, \ldots, \mathbf{k}_{1c})$. However in recent work with Loeser [16] we have shown that the varieties $E_i(c, d)$ sitting inside a suitable completion of the Grothendieck ring of algebraic varieties over $\mathbf{Q}$ are canonically associated to the cone integrals from which they are defined. The results with Loeser are based on the fundamental papers of Denef and Loeser [6] and [5] on motivic integration.

Theorem 5.1 shows how the behaviour of the zeta function $\zeta_{c, d, p}(s)$ and the function $f(n, p, c, d)$ as we vary p depends on the behaviour of the number of points in an associated set of varieties mod p. We make the following stronger conjecture about the behaviour of these zeta functions and hence the nature of the varieties $E_i(c, d)$, $i \in T(c, d)$:

Conjoncture **5.10.** — *For each c and d there exist finitely many rational functions $W_i(X, Y) \in \mathbf{Q}(X, Y)$ $(i = 1, \ldots, N)$ such that if $p \equiv i \bmod N$ then*

$$\zeta_{c, d, p}(s) = W_i(p, p^{-s}).$$

The rational functions $W_i(X, Y)$ *have the form*

$$W_i(X, Y) = \frac{P_i(X, Y)}{(1 - X^{a_{i1}}Y^{b_{i1}})...(1 - X^{a_{id_i}}Y^{b_{id_i}})}.$$

The nature of the denominator of $W_i(X, Y)$ will be a result of the fact that we are summing geometric progressions.

Note in particular that this conjecture implies the following:

Corollary **5.11.** — *Suppose Conjecture 5.10 is true. Then for* $n \in \mathbf{N}$ *and* $i = 1, ..., N$ *there exist polynomials* $r_{n,i}(X) \in \mathbf{Q}(X)$ *such that if* $p \equiv i \bmod N$ *then*

$$f(n, p, c, d) = r_{n,i}(p)$$

i.e. the function $f(n, p, c, d)$ *is PORC in* p.

Since $f(n, p, n-1, n) = f(n, p)$ this includes Higman's PORC conjecture as a special case. The proof that the conjecture implies PORC for the coefficients $f(n, p, c, d)$ of $\zeta_{c,d,p}(s)$ follows by expanding the rational function $W_i(X, Y)$ as

$$P_i(X, Y) \prod_{j=1}^{d_i} \left(\sum_{k=0}^{\infty} \left(X^{a_{ij}} Y^{b_{ij}} \right)^k \right)$$

and reading off the coefficient of Y^n.

We can actually deduce a stronger corollary from Conjecture 5.10 which gives some relationship between the polynomials $r_{n,i}(X)$ as we vary n.

Corollary **5.12.** — *Suppose Conjecture 5.10 is true. Let* $K_i = \mathbf{C}(X^{1/q_i})$ *be the field of rational functions in* X^{1/q_i} *where* $q_i = b_{i1} ... b_{id_i}$. *Then there exist positive rational numbers* $A_{i,k} \in \mathbf{Z}[1/q_i]$, *roots of unity* $\varsigma_{i,k}$ *and rational functions* $R_{i,k}(X, Z) \in K_i[Z]$ $(i = 1, ..., N, k = 1, ..., s_i)$ *which are polynomials in* Z *whose coefficients are rational functions in* X^{1/q_i} *such that if* $p \equiv i \bmod N$ *then*

$$f(n, p, c, d) = \sum_{k=1}^{s_i} R_{i,k}(p, n) \left(\varsigma_{i,k}\, p^{A_{i,k}} \right)^n.$$

Proof. — The proof is based on the same argument using partial fractions that shows that the coefficients a_n of a rational function in one variable are given by $a_n = \sum_{i=1}^{k} P_i(n)\gamma_i^n$ where P_i is a polynomial and γ_i is an algebraic integer (see for example [39] Theorem 4.1.1).

We can write $(1 - X^{a_{i1}}Y^{b_{i1}})...(1 - X^{a_{id_i}}Y^{b_{id_i}}) = \prod_{k=1}^{s_i}(1 - X^{A_{i,k}}\varsigma_{i,k}Y)^{c_k}$ where $(1 - X^{A_{i,k}}\varsigma_{i,k}Y)$ are coprime for different k and the $\varsigma_{i,k}$ are roots of unity. The theory

of partial fractions (see for example [25] Chapter V section 5) implies that there exist polynomials $P_{i,k}(Y) \in K_i[Y]$ for $k = 1, \ldots, s_i$ such that

$$W_i(X, Y) = \sum_{k=1}^{s_i} \frac{P_{i,k}(Y)}{(1 - X^{A_{i,k}} \varsigma_{i,k} Y)^{c_k}}.$$

Let $P_{i,k}(Y) = \sum_{j=0}^{M_{i,k}} P_{i,k,j}(X) Y^j$ where $P_{i,k,j}(X) \in K_i$. Setting

$$R_{i,k}(X, Z) = \sum_{j=0}^{M_{i,k}} P_{i,k,j}(X) \left(\varsigma_{i,k} X^{A_{i,k}}\right)^{-j} \binom{c_k + Z - 1 - j}{c_k - 1}$$

then by expanding the partial fractions in the expression for $W_i(X, Y)$ we see that the coefficient of Y^n is given by

$$\sum_{k=1}^{s_i} R_{i,k}(p, n) \left(\varsigma_{i,k} p^{A_{i,k}}\right)^n. \quad \square$$

One consequence of Theorem 5.1 is the following:

Theorem **5.13.** — *For each prime p there exist polynomials $P_p(Y)$ and $Q_p(Y)$ over $\mathbf{Z}$ whose degrees are bounded independently of p such that*

$$\zeta_{c,d,p}(s) = \frac{P_p(p^{-s})}{Q_p(p^{-s})}.$$

We can in fact use Theorem 5.13 to prove that the conjectured PORC behaviour of $f(n, p, c, d)$ actually implies Conjecture 5.10.

Theorem **5.14.** — *Suppose that for $n \in \mathbf{N}$ and $i = 1, \ldots, N$ there exist polynomials $r_{n,i}(X) \in \mathbf{Q}(X)$ such that if $p \equiv i \bmod N$ then*

$$f(n, p, c, d) = r_{n,i}(p).$$

Then Conjecture 5.10 is true.

Proof. — This is a consequence of Theorem 5.13 and the following observation made in Lemma 5.1 of [21]:

Proposition **5.15.** — *Let $\mathscr{P}$ be an infinite set of primes and let $(a_n(X))_{n \in \mathbf{N}}$ be a sequence of rational functions over $\mathbf{Q}$. Suppose that for each $p \in \mathscr{P}$ there exist polynomials $P_p(Y)$ and $Q_p(Y)$*

in $\mathbf{Q}[Y]$ *such that*

$$\sum_{n=0}^{\infty} a_n(p)Y^n = \frac{P_p(Y)}{Q_p(Y)},$$

and that the degrees of P_p *and* Q_p *are bounded for all* $p \in \mathscr{P}$. *Then there exists a rational function* $W(X, Y) \in \mathbf{Q}(X, Y)$ *such that*

$$\frac{P_p(Y)}{Q_p(Y)} = W(p, Y)$$

for all $p \in \mathscr{P}$.

Recall at the end of the previous section we predicted that the analysis of the integral describing these rational functions would fall into two parts:

(1) analysing the good basis for normal subgroups in the free nilpotent group; and

(2) analysing the measure of certain sets in the algebraic automorphism group.

In [21] the following conjecture was made in relation to the first of these problems:

Conjecture **5.16.** — *Let* F *be a finitely generated free nilpotent group of class c on d generators. Then there exists a rational function* $W(X, Y) \in \mathbf{Q}(X, Y)$ *such that for almost all primes p*

$$\zeta_{F,p}^{\triangleleft}(s) = W(p, p^{-s}).$$

So a proof of Conjecture 5.16 will probably form an essential stepping stone to a proof of Conjecture 5.10 and hence Higman's PORC conjecture. This connection gives a much greater significance to the original Conjecture 5.16 than was first supposed. In the original paper [21] where Conjecture 5.16 was made, a proof is given for class 2 free nilpotent groups. The proof combines Proposition 5.15 with properties of Hall polynomials. In joint work with Grunewald [15] we have established this conjecture for 2-generator free nilpotent groups of arbitrary class. We collect together our present knowledge in the following:

Proposition **5.17.** — *Conjecture 5.16 is true for*

(a) *class* 2 *free nilpotent groups [21]; and*

(b) 2*-generator free nilpotent groups [15].*

It is a simple observation to see that a finite number of exceptional primes are covered by residue classes by taking N in Conjecture 5.10 to be divisible by these primes. The same argument implies that a function which is PORC on almost all primes is PORC on all primes.

The evidence that we documented in the Introduction certainly means that we are going to expect some genuine PORC behaviour in Conjecture 5.10 and Corollary 5.16. In other words, there won't be just one rational function or polynomial in general that will work for almost all primes. Since Conjecture 5.16 implies that the behaviour of normal subgroups in free nilpotent groups will not give rise to a genuine PORC behaviour, we are expecting the analysis of (2) above to provide this.

One approach to proving the strong uniformity statement of Conjecture 5.10 would be to understand the polynomial $F_{\mathscr{L}}(X)$ associated to the free nilpotent Lie algebra and the associated varieties $E_{i,c,d}$ ($i \in T(c, d)$). Counting points mod p in affine space or on flag varieties is uniform in p. Counting solutions to $Y^n = 1 \bmod p$ displays a more PORC behaviour depending on the residue class of p mod n. Is it possible to prove that the varieties $E_{i,c,d}$ ($i \in T(c, d)$) and their intersections are built from such varieties?

In [14] we showed that for an arbitrary nilpotent group G, the zeta function $\zeta^{\triangleleft}_{G,p}(s)$ (and the zeta function $\zeta_{G,p}(s)$ counting all subgroups although this is not so relevant for us here) are given by cone integrals. We therefore have an explicit formula given by Theorem 5.4 for $\zeta^{\triangleleft}_{G,p}(s)$. The following example shows that it is possible to realise the elliptic curve $Y^2 = X^3 - X$ as an intersection of varieties in the explicit expression for $\zeta^{\triangleleft}_{G,p}(s)$.

Theorem **5.18.** — *Let* G *be the Hirsch length* 9, *class two nilpotent group given by the following presentation:*

$$G = \left\langle \begin{array}{c} x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3 : [x_1, x_4] = y_3, [x_1, x_5] = y_1, [x_1, x_6] = y_2 \\ [x_2, x_4] = y_2, [x_2, x_6] = y_1, [x_3, x_4] = y_1, [x_3, x_5] = y_3 \end{array} \right\rangle$$

where all other commutators are defined to be 1. *Let* E *be the elliptic curve* $Y^2 = X^3 - X$. *Then there exist two non-zero rational functions* $P_1(X, Y)$ *and* $P_2(X, Y) \in \mathbf{Q}(X, Y)$ *such that for almost all primes* p :

$$\zeta^{\triangleleft}_{G,p}(s) = P_1(p, p^{-s}) + \mathrm{card}(E(\mathbf{F}_p))P_2(p, p^{-s}).$$

To see where the elliptic curve is hidden in this presentation, take the determinant of the 3×3 matrix (a_{ij}) with entries $a_{ij} = [x_i, x_{j+3}]$ and you will get the projective version of E. When $p \equiv 3 \bmod 4$, $\mathrm{card}(E(\mathbf{F}_p)) = p + 1$. However the behaviour of the number of points on the elliptic curve $Y^2 = X^3 - X \bmod p$ for $p \equiv 1 \bmod 4$ is certainly not uniform but varies wildly with the prime. For a description of the behaviour of $\mathrm{card}(E(\mathbf{F}_p))$ see, for example, Chapter 18.4 of [24]. This example appears in [10]

and [11]. It answers negatively the following question posed in [21] which was a generalization of Conjecture 5.16 for arbitrary nilpotent groups:

Question. — Let G be a finitely generated nilpotent group. Do there exist finitely many rational functions $W_1(X, Y), ..., W_r(X, Y) \in \mathbf{Q}(X, Y)$ such that for all primes p there exists some $i \in \{1, ..., r\}$ and

$$\zeta^{\triangleleft}_{G,p}(s) = W_i(p, p^{-s})?$$

So Theorem 5.18 indicates that a positive answer to Conjecture 5.16 will be something special about free nilpotent groups.

6. Asymptotic growth of finite nilpotent groups

In this section we prove the following:

Theorem **6.1.** — *For integers n, c, d define $g(n, c, d)$ to be the number of finite nilpotent groups (up to isomorphism) of order n of class at most c generated by at most d generators. Then there exist a rational number $\alpha(c, d) \in \mathbf{Q}$, an integer $\beta(c, d) \geqslant 0$ and $\gamma(c, d) \in \mathbf{R}$ such that*

$$g(1, c, d) + \cdots + g(n, c, d) \sim \gamma(c, d) \cdot n^{\alpha(c,d)} (\log n)^{\beta(c,d)}.$$

We recall the following definition from [14]:

Definition **6.2.** — *We say that a function $Z(s)$ is defined as an Euler product of cone integrals over $\mathbf{Q}$ with cone integral data $\mathscr{D}$ if*

$$Z(s) = Z_{\mathscr{D}}(s) = \prod_{p \text{ prime}} \left(a_{p,0}^{-1} \cdot Z_{\mathscr{D}}(s, p) \right)$$

where $a_{p,0} = Z_{\mathscr{D}}(\infty, p)$ is the constant coefficient of $Z_{\mathscr{D}}(s, p)$, i.e. we normalize the local factors to have constant coefficient 1.

We proved in [14] the following Theorem about such Euler products of cone integrals:

Theorem **6.3.** — *Let $Z(s)$ be defined as an Euler product of cone integrals over $\mathbf{Q}$. Then $Z(s)$ is expressible as a Dirichlet series $\sum_{m=1}^{\infty} a_m m^{-s}$ with non-negative coefficients a_m.*

(1) *The abscissa of convergence α of $Z(s)$ is a rational number and $Z(s)$ has a meromorphic continuation to $\mathrm{Re}(s) > \alpha - \delta$ for some $\delta > 0$.*

(2) *Let the pole at $s = \alpha$ have order w. Then there exists some real number $\gamma \in \mathbf{R}$ such that*

$$a_1 + \cdots + a_m \sim \gamma \cdot m^{\alpha} (\log m)^{w-1}.$$

We have already proved that the zeta function $\zeta_{c,d}(s)$ defined as the Dirichlet series with coefficients $g(n, c, d)$ has the following Euler product (Corollary 2.9):

$$\zeta_{c,d}(s) = \prod_{p \text{ prime}} \zeta_{c,d,p}(s).$$

We have also established in Theorem 5.7 that for almost all primes p

$$\zeta_{c,d,p}(s) = c_p^{-1}(1 - p^{-1})^{-n} Z_{\mathscr{D}_{c,d}}(s - n, p)$$

where $\mathscr{D}_{c,d}$ denotes the cone integral data in Theorem 5.7. Since the constant coefficient of $\zeta_{c,d,p}(s)$ is 1, we have that the constant coefficient $a_{p,0}$ of the cone integral $Z_{\mathscr{D}_{c,d}}(s, p)$ is $c_p(1 - p^{-1})^n$.

Theorem 6.1 therefore follows from Theorem 6.3 (2).

We also record the following corollary about the analytic behaviour of $\zeta_{c,d}(s)$ which is a consequence of Theorem 6.3 (1):

Corollary **6.4.** — *The abscissa of convergence* $\alpha(c, d)$ *of* $\zeta_{c,d}(s)$ *is a rational number and* $\zeta_{c,d}(s)$ *has a meromorphic continuation to* $\mathrm{Re}(s) > \alpha - \delta$ *for some* $\delta > 0$.

A number of interesting problems now arise from Theorem 6.1:

Problem **1.** — Determine for a given c and d the values of the rational numbers $\alpha(c, d)$ and $\beta(c, d)$.

The number $\alpha(c, d)$ is the abscissa of convergence of the associated zeta function $\zeta_{c,d}(s) = \sum_{n=1}^{\infty} g(n, c, d)n^{-s}$ whilst $\beta(c, d) + 1$ is the order of the pole that exists at $s = \alpha(c, d)$.

In [14] we proved a similar result to Theorem 6.1 for counting normal subgroups inside an arbitrary finitely generated nilpotent group:

Theorem **6.5.** — *Let* G *be a finitely generated nilpotent infinite group. Then there exist a rational number* $\alpha^{\triangleleft}(G) \in \mathbf{Q}$, *a non-negative integer* $\beta^{\triangleleft}(G) \geqslant 0$ *and some real number* $\gamma^{\triangleleft}(G) \in \mathbf{R}$ *such that*

$$s_n^{\triangleleft}(G) \sim \gamma^{\triangleleft}(G) \cdot n^{\alpha^{\triangleleft}(G)} (\log n)^{\beta^{\triangleleft}(G)}$$

where $s_n^{\triangleleft}(G)$ *is the number of normal subgroups of index bounded by* n.

Problem **2.** — What is the relationship between $\alpha(c, d)$ and $\beta(c, d)$ and $\alpha^{\triangleleft}(F_{c,d})$ and $\beta^{\triangleleft}(F_{c,d})$ where $F_{c,d}$ is the free nilpotent group of class c on d generators?

It is clear that $\alpha^{\triangleleft}(F_{c,d}) \geqslant \alpha(c, d)$ since $g(n, c, d)$ is counting normal subgroups of index n in $F_{c,d}$ up to some equivalence. When $c = 1$, i.e. counting finite abelian groups,

then $\alpha^{\triangleleft}(F_{1,d}) = d$ and $\beta^{\triangleleft}(F_{1,d}) = 0$ whilst $\alpha(1, d) = 1$ and $\beta(1, d) = 0$. There is not so much progress yet even in determining the values of $\alpha^{\triangleleft}(F_{c,d})$ and $\beta^{\triangleleft}(F_{c,d})$ for $c > 1$. The following proposition collects together our present knowledge, all proved in [21]:

Proposition **6.6.** — *Let n denote the Hirsch length of* $F_{c,d}$.

(1) $d \leqslant \alpha^{\triangleleft}(F_{c,d}) \leqslant n$.

(2) *If* $c = 2$ *then* $(d^3 - d^2 + 2)/4d \leqslant \alpha^{\triangleleft}(F_{2,d}) \leqslant \max\{d, (d-1)(d+1)/2\}$.

(3) $\alpha^{\triangleleft}(F_{2,2}) = 2$ *and* $\beta^{\triangleleft}(F_{2,2}) = 0$.

(4) $\alpha^{\triangleleft}(F_{2,3}) = 3$ *and* $\beta^{\triangleleft}(F_{2,3}) = 0$.

We have proved that $\zeta_{c,d}(s)$ has some meromorphic continuation beyond its region of convergence. It should be pointed out that in general zeta functions associated to groups cannot be meromorphically continued to the whole complex plane but in general have natural boundaries. For the proof we refer to [12]. For example, the following result is proved there:

Theorem **6.7.** — $\zeta^{\triangleleft}_{F_{2,3}}(s)$ *can be meromorphically continued beyond its region of convergence* $\mathrm{Re}(s) > 3$ *to* $\mathrm{Re}(s) > 7/5$. *However* $\mathrm{Re}(s) = 7/5$ *is a natural boundary for* $\zeta^{\triangleleft}_{F_{2,3}}(s)$ *beyond which no further meromorphic continuation is possible.*

Problem **3.** — Does $\zeta_{c,d}(s)$ in general have a natural boundary beyond which meromorphic continuation is not possible?

Finally there is the question of explicitly calculating examples:

Problem **4.** — Calculate explicit examples of $\zeta_{c,d}(s)$ and $\zeta_{c,d,p}(s)$. *

Currently explicit calculations have been made of $\zeta^{\triangleleft}_{F_{2,2}}(s)$ and $\zeta^{\triangleleft}_{F_{2,3}}(s)$ (see [21]):

$$\zeta^{\triangleleft}_{F_{2,2}}(s) = \zeta(s)\zeta(s-1)\zeta(3s-2)$$

$$\zeta^{\triangleleft}_{F_{2,3}}(s) = \zeta(s)\zeta(s-1)\zeta(s-2)\zeta(3s-5)\zeta(5s-8)\zeta(6s-9)\prod_{p \text{ prime}} W(p, p^{-s})$$

where $W(X, Y) = (1 + X^3Y^3 + X^4Y^3 + X^6Y^5 + X^7Y^5 + X^{10}Y^8)$ and $\zeta(s)$ is the Riemann zeta function.

---

* Note added in proof: My Ph.D. student Christopher Voll has proved the following:

$$\zeta_{2,2}(s) = \zeta(s)\zeta(2s)\zeta(3s)^2\zeta(4s).$$

Part II. Counting finite p-groups of coclass r and Conjecture P

7. Rationality of the zeta function counting p-groups of coclass r

Definition **7.1.** — *A p-group of order p^n and nilpotency class c is said to have coclass $r = n - c$. A pro-p group of coclass r is an inverse limit of an infinite chain of epimorphisms of finite p-groups of coclass r.*

This generalizes the concept of maximal class, studied extensively by Blackburn [1], which corresponds to coclass 1.

Definition **7.2.** — *Let $c(r, n, p)$ denote the number of groups (up to isomorphism) of order p^n and coclass r and define the zeta function of p-groups of coclass r to be*

$$\zeta_{\mathrm{ccl}}^{r,p}(s) = \sum_{n=0}^{\infty} c(r, n, p)p^{-ns}.$$

In this section we prove Theorem 1.12 that $\zeta_{\mathrm{ccl}}^{r,p}(s)$ is a rational function in p^{-s}.

When one considers p-groups of a fixed class c generated by d generators (as we did in Part I) then there is a free object whose finite images give all such groups, namely the free nilpotent pro-p group of class c on d generators. For this part of the paper put $\mathrm{F}_{c,d} = \mathrm{F}_d/\gamma_{c+1}(\mathrm{F}_d)$, where F_d is the free d-generator pro-p group.

When we come to consider finite p-groups of coclass r then such a free object does not exist. However, using the knowledge we have of p-groups of a given coclass from Conjectures A-E, we can define a "small" group such that all finite p-groups of coclass r appear as finite quotients of this group. There are finite quotients which have coclass bigger than r; but small here is meant to mean that we don't have to take the free pro-p group as our choice, but rather we can use a p-adic analytic group which is free in some variety. Let us state a version of Conjecture A and a related result (proofs of which can be found in the papers by Leedham-Green [29] and Shalev [37]) which will allow us to define explicitly the "universal" group for p-groups of coclass r.

Theorem **7.3.** *(Conjecture A) — There exists a positive integer $g = g(p, r)$ such that every p-group of coclass r has a normal subgroup of class at most 2 (1, if $p = 2$) and index dividing p^g.*

Theorem **7.4.** *(Proposition 4.5 of [37]) — There exists a positive integer $h = h(p, r)$ such that for every p-group of coclass r, if $n > h$ then*

$$|\gamma_n(\mathrm{G})/\gamma_{n+1}(\mathrm{G})| \leqslant p.$$

A p-group of coclass r is generated by at most $r+1$ elements. (If $d(G)=d$ then $p^d=|G/\Phi(G)|\leqslant|G/\gamma_2(G)|\leqslant p^{n-(c-1)}=p^{r+1}$.)

Definition **7.5.** — *Define the group* $\mathcal{U}_r$ *by*

$$\mathcal{U}_r=F_{r+1}/\gamma_3\left(\gamma_g(F_{r+1})\cdot F_{r+1}^{p^g}\right).$$

The following is then a Corollary of Theorem 7.3:

Corollary **7.6.** — *Every finite p-group of coclass r is an image of* $\mathcal{U}_r$.

We remark that every subgroup of finite index in the finitely generated pro-p group $\mathcal{U}_r$ is open (see Chapter 1 of [7]) so we need not distinguish between finite images in the category of groups and in the category of pro-p groups.

Note that the group $\mathcal{U}_r$ is a finite extension of a class two finitely generated nilpotent pro-p group, and hence is a p-adic analytic pro-p group. It is also a free pro-$\mathcal{C}$ group for an almost full family of finite groups $\mathcal{C}$ as defined in Definition 2.4. Let $\mathfrak{G}=\mathrm{Aut}(\mathcal{U}_r)$. Then by our analysis of sections 2 and 3 we proved that the zeta function counting finite images up to isomorphism could be expressed as:

$$\begin{aligned}\zeta_{\mathcal{G}(\mathcal{U}_r)}(s)&=\zeta_{\widetilde{\mathcal{X}(\mathcal{U}_r)}}(s)\\&=\sum_{H\lhd\mathcal{U}_r}|\mathcal{U}_r:H|^{-s}|\mathfrak{G}:\mathrm{Stab}_{\mathfrak{G}}(H)|^{-1}.\end{aligned}$$

By choosing a suitable subgroup $\mathcal{N}\times\mathfrak{G}_1$ of finite index in $\mathcal{U}_r\times\mathfrak{G}$, namely a characteristic open uniform subgroup, we proved in section 3 how to represent this zeta function as a sum of $\mathcal{L}_G$-definable integrals

$$cc'\int_{\mathcal{M}(K,\mathfrak{K})}F(\mathbf{g})F'(\mathbf{x})d\mu d\nu$$

for each pair of subgroups $(K,\mathfrak{K})$ with $\mathcal{N}\leqslant K\leqslant\mathcal{U}_r$ and $\mathfrak{G}_1\leqslant\mathfrak{K}\leqslant G$ (see (2) of section 3). Recall

$$\mathcal{M}(K,\mathfrak{K})=\bigcup_{H\in\mathcal{X}(\mathcal{U}_r,K,\mathfrak{K})}M(H)\times N(H)\subset\mathcal{N}^{(d+n)}\times\mathfrak{G}_1^{(r+t)}$$

where $M(H)$ consists of bases for the normal subgroup H and $N(H)$ consists of bases for the stabilizer of H in $\mathfrak{G}$. However, as we pointed out, $\mathcal{U}_r$ has finite images that do not have coclass r. So we want to include an extra statement in the definable integrals expressing $\zeta_{\mathcal{G}(\mathcal{U}_r)}(s)$ to exclude those normal subgroups giving rise to these unwanted

images and hence represent the following:

$$\zeta^{r,p}_{\mathrm{ccl}}(s) = \sum_{\mathrm{H} \in \mathscr{X}_r} |\mathscr{U}_r : \mathrm{H}|^{-s} |\mathfrak{G} : \mathrm{Stab}_{\mathfrak{G}}(\mathrm{H})|^{-1}$$

where $\mathscr{X}_r = \left\{ \mathrm{H} : \mathrm{H} \lhd \mathscr{U}_r,\ \mathscr{U}_r/\mathrm{H} \text{ has coclass } r \right\}$ as a sum of $\mathscr{L}_G$-definable integrals

$$cc' \int_{\mathscr{M}_r(\mathrm{K}, \mathfrak{K})} \mathrm{F}(\mathbf{g})\mathrm{F}'(\mathbf{x}) d\mu d\nu$$

where

$$\mathscr{M}_r(\mathrm{K}, \mathfrak{K}) = \bigcup_{\mathrm{H} \in \mathscr{X}(\mathscr{U}_r, \mathrm{K}, \mathfrak{K}) \cap \mathscr{X}_r} \mathrm{M}(\mathrm{H}) \times \mathrm{N}(\mathrm{H}).$$

We therefore have to demonstrate that we have a definable formula on the basis of a subgroup H to say that it defines a finite image of coclass r. In contrast to the class of a group, coclass looks at first sight rather undefinable: as the size of the group increases, so must the class of the group if the coclass is to remain bounded. Therefore it appears that one might require checking commutators of increasing length which cannot be captured in a definable way. However we are going to exploit Theorem 7.4 which tells us that coclass is in fact determined in the first $h(p, r)$ layers of the lower central series.

For a normal subgroup H of $\mathscr{U}_r$, define integers $d(\mathrm{H}, i)$ by

$$\left| \gamma_i\left(\mathscr{U}_r\right) \mathrm{H} / \gamma_{i+1}\left(\mathscr{U}_r\right) \mathrm{H} \right| = p^{d(\mathrm{H}, i)}.$$

Then, by Theorem 7.4, $\mathscr{U}_r/\mathrm{H}$ has coclass r if and only if $d(\mathrm{H}, 1) + \cdots + d(\mathrm{H}, h(p, r)) = r + h(p, r)$ and, for all $i > h(p, r)$, $d(\mathrm{H}, i) \leqslant 1$.

Lemma **7.7.** — *For all* $i > h(p, r)$, $d(\mathrm{H}, i) \leqslant 1$ *if and only if for all normal subgroups* L *of* $\mathscr{U}_r$ *with* $\left(\gamma_{h(p,r)+1}\left(\mathscr{U}_r\right) \mathrm{H}\right) \geqslant \mathrm{L} \geqslant \mathrm{H}$, *if* K *is a subgroup with* $\mathrm{L} \geqslant \mathrm{K} \geqslant [\mathscr{U}_r, \mathrm{L}]\mathrm{H}$ *then either* $\mathrm{K} = \mathrm{L}$ *or* $[\mathscr{U}_r, \mathrm{L}]\mathrm{H}$.

Proof. — The "if" follows because these are p-groups, so if $d(\mathrm{H}, i) > 1$, it would be possible to fit a subgroup K strictly between $\gamma_i\left(\mathscr{U}_r\right) \mathrm{H}$ and $\gamma_{i+1}\left(\mathscr{U}_r\right) \mathrm{H}$; the "only if" follows since if L is normal then it must actually be one of the terms of the lower central series $\gamma_i\left(\mathscr{U}_r\right) \mathrm{H}$. □

Lemma **7.8.** — *The statement:*

> *"for all normal subgroups* L *of* $\mathscr{U}_r$ *with* $\gamma_{h(p,r)+1}\left(\mathscr{U}_r\right) \mathrm{H} \geqslant \mathrm{L} \geqslant \mathrm{H}$, *if* K *is a subgroup with* $\mathrm{L} \geqslant \mathrm{K} \geqslant [\mathscr{U}_r, \mathrm{L}]\mathrm{H}$ *then either* $\mathrm{K} = \mathrm{L}$ *or* $[\mathscr{U}_r, \mathrm{L}]\mathrm{H}$"

is a definable sentence.

Proof. — Firstly it is possible to quantify over all normal subgroups by quantifying over their bases; also to say that $L \geqslant H$, for example, just requires the statement that it is possible to write a basis for H in terms of the basis for L. Finally we just need to check that $\gamma_{h(p,r)+1}\left(\mathscr{U}_r\right)$ and $[\mathscr{U}_r, L]$ are definable. The first group is a fixed subgroup so we can choose a fixed basis for it. As for the second we can put a definable condition on a basis that it be a basis for $[\mathscr{U}_r, L]$: firstly the group it generates must contain each commutator of the form $[g, l]$ with $g \in \mathscr{U}_r$ and $l \in L$, and secondly it must be minimal with respect to this condition. □

Finally we come to showing:

Lemma **7.9.** — *The statement "*$d(H, 1) + \cdots + d(H, h(p, r)) = r + h(p, r)$*" is definable.*

Proof. — The statement $|\mathscr{U}_r/\gamma_{h(p,r)+1}\left(\mathscr{U}_r\right) H| = p^{r+h(p,r)}$ is equivalent to the existence of a chain of subgroups

$$\mathscr{U}_r = K_0 \gneqq K_1 \gneqq \ldots \gneqq K_{r+h(p,r)-1} \gneqq K_{r+h(p,r)} = \gamma_{h(p,r)+1}\left(\mathscr{U}_r\right) H$$

such that if $K_j \geqslant K \geqslant K_{j+1}$ then $K = K_j$ or K_{j+1}. Since $\gamma_{h(p,r)+1}\left(\mathscr{U}_r\right)$ is a fixed subgroup we can fix a basis for it. Hence everything is definable. □

Putting all these pieces together we get that coclass is definable and hence that the subsets $\mathscr{M}_r(K, \mathfrak{K})$ are definable subsets. This completes the proof that $\zeta^{r,p}_{\mathrm{ccl}}(s)$ can be represented by an $\mathscr{L}_G$-definable integral. By [8], it is therefore a rational function in p^{-s} and Theorem 1.12 follows. □

8. Periodicity and Conjecture P

To describe precisely the statement of Conjecture P we quote the following three paragraphs (with some changes) from the introduction of [32].

In [28] a directed graph $\mathscr{G}_p$ was defined on all p-groups. Its vertices are all p-groups for a fixed prime p, one for each isomorphism type, and its edges are the pairs (P, Q) with P isomorphic to the quotient $Q/\gamma_c(Q)$ where $\gamma_c(Q)$ is the last non-trivial term of the lower central series of Q. If (P, Q) is an edge of $\mathscr{G}_p$, then Q is an *immediate descendant* of P. R is a *descendant* of P if there is a possibly empty path from P to R. A group is *extendable* if it has immediate descendants and otherwise it is *terminal*. (Originally Newman and O'Brien called extendable groups by the name *capable*; however as Avinoam Mann has pointed out to me, capable was already used by Philip Hall for groups which are central factor groups of some group.) The *descendant tree* $\mathscr{T}_P$ of P is the subgraph of its descendants. A group of class c is *infinitely extendable* if it has descendants of all classes greater than c.

A finite p-group is called *coclass settled* if all its descendants have the same coclass. In [37] Shalev proved that 2-groups of coclass r are coclass settled by class 2^{r+3} and for p odd, that p-groups of coclass r are coclass settled by class $2p^r$. This is precisely Theorem 7.4 that we have been using in the previous section. Note that an immediate descendant of a coclass settled group of order p^n must have order p^{n+1}.

We can associate with each pro-p group G of coclass r a family of finite p-groups of coclass r in the following way. All the finite quotients of G have coclass at most r. By Shalev's result, all but finitely many of these are coclass settled and have coclass r. Since there are only finitely many pro-p groups of coclass r (Conjecture D), all but finitely many of the coclass settled finite quotients are quotients of only one pro-p group. These finite quotients form an infinite chain. The family $\mathscr{F}_G$ associated with the pro-p group G is the tree of descendants of the smallest group R_G in the chain. We call R_G the *root* of the family. An infinitely extendable descendant of a root is *mainline*. It follows from [29] that all but finitely many p-groups of coclass r belong to some family. Because the p-groups in a family are all coclass settled, each direct descendant of a group of order p^n has order p^{n+1}.

For example, it is known that there is exactly one family of p-groups of coclass 1 for every prime.

Call a connected subgraph of a family $\mathscr{F}_G$ a *twig* if it includes at most one mainline group. One formulation of Conjecture A for the prime $p=2$ implies that there is bound on the length of twigs in a family. This is known to be false for primes $p > 2$. In two papers [26] and [27], Leedham-Green and McKay proved that the unique family of coclass 1 5-groups has twigs of length m emanating from the mth point on the mainline. A full description of the tree has been conjectured by Newman based on computer calculations and appears in [31].

In [32] a certain periodicity is predicted in these trees for 2-groups of finite coclass where the twig lengths are bounded. The descendant tree $\mathscr{T}_P$ of a p-group P is *periodic* if P has a proper descendant Q such that $\mathscr{T}_Q$ is isomorphic to $\mathscr{T}_P$. The *period* of a periodic $\mathscr{T}_P$ is the least value of $\log_p(|Q|/|P|)$ and the *descendant pattern* of $\mathscr{T}_P$ is $\mathscr{T}_P - \mathscr{T}_Q$. We call a tree *ultimately periodic* if it contains a descendant tree which is periodic.

Newman and O'Brien, based on experimental evidence, have made the following:

Conjecture **P.** — *Each family of 2-groups of coclass r contains a group* R *and a proper descendant* Q *of order $2^q|R|$ where q divides 2^{r-1} such that the descendant tree of* Q *is isomorphic to the descendant tree of* R.

The conjecture is part of four conjectures about 2-groups: Conjectures P, Q, R and S. The other conjectures concern specific bounds for the size of the periodic root, the minimal R satisfying Conjecture P, (Conjecture R), the size of sporadic groups (Conjecture S) and the size of groups to guarantee being coclass settled (Conjecture Q).

Their conjectures are actually made for a slight refinement of coclass that they call "lower exponent p-coclass". This measures p-groups against the lower p-series rather than the lower central series. Recall from [7] the definition of the lower p-series $P_i(G) : P_1(G) = G$ and $P_{i+1}(G) = [P_i(G), G]P_i(G)^p$ for $i > 1$. In [32] the filtration is shifted by 1, since they define $P_0(G) = G$, but we prefer to stick to the definition given here, not least because it compares better with the lower central series. The *lower exponent p-coclass* of a p-group P is then defined to be $n - c$ where $|P| = p^n$ and c is the lower exponent p-class defined by $P_c(G) \neq 1$ but $P_{c+1}(G) = 1$. The coclass r in Conjecture P is actually the lower exponent p-coclass.

In this section we are going to be concerned with proving the qualitative rather than the quantitative side of Conjecture P so the order of periodicity will not concern us. We are also going to stick with the original definition of coclass, rather than deal with lower exponent p-coclass. In Theorem 6.1 of [32] it is proved that a p-group of coclass r and order at least p^{8p^r+r} has lower exponent p-coclass r. Hence our proof will cover those families of p-groups of lower exponent p-coclass r which also have coclass r since the trees are the same. (Recall that the root of the tree is a coclass settled group.) These are the families which arise from pro-p groups which are uniserial p-adic space groups. The additional pro-p groups (and hence trees) that one gets by considering lower exponent p-coclass are described in Lemma 2.2 of [32] where the following is proved:

Proposition **8.1.** — *A finitely generated pro-p group of lower exponent p-coclass r is either a central extension of a cyclic subgroup of order p by a pro-p group of lower exponent p-coclass* $r - 1$ *or a uniserial p-adic space group.*

Note for example that there is only one family of 2-groups of coclass 1. It has root D_8 and each mainline group has three immediate descendants, one mainline and the other two terminal corresponding respectively to the dihedral group, quaternion group and semi-dihedral group. This is however one of two families of 2-groups of lower exponent p-coclass 1, the other has root $C_2 \times C_4$ and two groups of order 2^n for every $n \geqslant 4$.

Since Conjecture A holds for lower exponent p-coclass, all the arguments of the previous section and this section will go through with the lower central series $\gamma_i(G)$ replaced by the lower p-series $P_i(G)$ which is also definable.

As we mentioned above, for primes $p > 2$, twig lengths are not necessarily bounded so we will not expect Conjecture P to hold as written. However Newman's conjectured shape of the tree of 5-groups of coclass 1 does have a more complex notion of periodicity, which consists of some periodicity down the twigs. We consider in section 9 the example of 5-groups of coclass 1.

Here we prove the qualitative version of Conjecture P for 2-groups and a periodicity result for odd primes which captures some of the nature of the periodicity down twigs.

Definition **8.2.** — *For a family* $\mathscr{F}_G$ *and an integer* M *define* $\mathscr{F}_G(M)$ *to be the subtree consisting of all mainline groups and non-mainline groups of distance at most* M *from a mainline group.*

So for $p=2$, there exists M such that $\mathscr{F}_G(M)=\mathscr{F}_G$. We prove the following:

Theorem **8.3.** — *Let* $\mathscr{F}_G$ *be a family of p-groups of coclass r and let* $M \geqslant 0$ *be an integer. Then* $\mathscr{F}_G(M)$ *is ultimately periodic.*

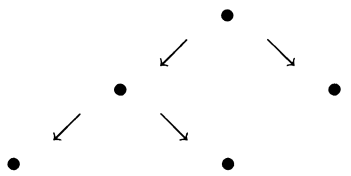
We are going to use the zeta functions of the previous section as a tool. To that end, for each tree $\mathscr{F}_G$, define a zeta function as follows:

$$\zeta_{\mathscr{F}_G}(s) = \sum_{P \in \mathscr{F}_G} |P|^{-s}$$
$$= \sum_{n=0}^{\infty} c(r, n, p, \mathscr{F}_G) p^{-ns}.$$

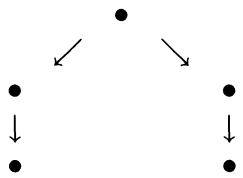
The second line is a definition of the coefficient $c(r, n, p, \mathscr{F}_G)$ which counts the number of p-groups of coclass r of order p^n in the family $\mathscr{F}_G$. We shall prove

Theorem **8.4.** — *For each family* $\mathscr{F}_G$ *of p-groups of coclass r,* $\zeta_{\mathscr{F}_G}(s)$ *is a rational function in* p^{-s}.

For 2-groups, the periodicity conjecture certainly implies this rationality result. But of course not conversely. Rationality just says something about the numbers of groups at each level and nothing about the shape. For example, let T_0 be the graph



and T_1 be the graph



Then to each infinite sequence $\theta = (\theta_n)$ with $\theta_n = 0$ or 1, we define a tree with one infinite branch and a twig of type T_{θ_n} emanating from the nth node in this branch. The zeta function corresponding to this tree is always rational but periodicity only occurs if the sequence θ is periodic.

So we are going to introduce a slightly more subtle zeta function which takes into account the shape of the twigs. Given any group in a family $\mathscr{F}_G$ there is a bound $N(\mathscr{F}_G)$ on the number of direct descendants. One way to see this is to recall that each p-group P in the tree is determined by a normal subgroup N of finite index in $\mathscr{U}_r$, a p-adic analytic group. Now the number of direct descendants of a group is therefore bounded by the number of normal subgroups of index p in N. Since $\mathscr{U}_r$ is p-adic analytic, it has bounded rank and hence there is a bound on the number of generators of finite index subgroups (see Chapter 4 of [7]). This implies that there is a bound on the number of such index p normal subgroups.

Let $\mathfrak{T}(M, N(\mathscr{F}_G))$ be the set of finite (directed) trees of length bounded by M with a unique root and the valency of each node bounded by $N(\mathscr{F}_G)$. Clearly $\mathfrak{T}(M, N(\mathscr{F}_G))$ is finite. Now a family $\mathscr{F}_G$ consists of an infinite chain made up of the mainline groups which we shall denote P_n. From each mainline group P_n define the twig $t_n(M)$ to be the directed graph with unique root P_n together with all non-mainline groups of distance at most M from P_n. Then for each $t \in \mathfrak{T}(M, N(\mathscr{F}_G))$ define a zeta function

$$\zeta_{\mathscr{F}_G, M, t}(s) = \sum_{t_n(M) = t} |P_n|^{-s}$$
$$= |P_1|^{-s} \sum_{t_n(M) = t} p^{-(n-1)s}.$$

Theorem **8.5.** — *$\mathscr{F}_G(M)$ is ultimately periodic if and only if for all $t \in \mathfrak{T}(M, N(\mathscr{F}_G))$, $\zeta_{\mathscr{F}_G, M, t}(s)$ is a rational function in p^{-s}.*

Proof. — A power series $\sum_{n=0}^{\infty} a_n T^n$ is a rational function in T if and only if the coefficients a_n satisfy a linear recurrence relation of length d, say, with constant coefficients. If the a_n are a bounded set of positive integers then this is equivalent to the coefficients a_n being periodic for n large enough. This follows because there are only finitely many different sequences $a_n, \ldots, a_{n+d-1}$, hence for some $s < t$ we have $a_{s+i} = a_{t+i}$ for $0 \leqslant i \leqslant d-1$ and so a_n has period $\leqslant t - s$. In our case the coefficients a_n are just 1 or 0 according to whether the twig of P_n of length M is isomorphic to t or not. □

Therefore Theorem 8.3 will be a corollary of the following:

Theorem **8.6.** — *$\zeta_{\mathscr{F}_G, M, t}(s)$ is a rational function in p^{-s}.*

The strategy for the proof of both Theorems 8.4 and 8.6 is to take the definable integral describing the number of all p-groups of coclass r and to add more definable

conditions so that we are only counting p-groups in the family $\mathscr{F}_G$ and finally only those which are mainline with twigs of a certain shape.

The pro-p group G is the inverse limit of the p-groups P_n in the mainline of $\mathscr{F}_G$. Let $\mathscr{P}$ denote a choice of normal subgroup in $\mathscr{U}_r$ such that $\mathscr{U}_r/\mathscr{P} \cong G$. For $n \geqslant 1$, let $\mathscr{P}_n \geqslant \mathscr{P}$ denote the normal subgroup with $\mathscr{U}_r/\mathscr{P}_n \cong P_n$. Then

Lemma **8.7.**

$$\zeta_{\mathscr{F}_G}(s) = \sum_{H \in \mathscr{X}(\mathscr{F}_G)} |\mathscr{U}_r : H|^{-s} |\mathfrak{G} : \mathrm{Stab}_{\mathfrak{G}}(H)|^{-1}$$

where

$$\mathscr{X}(\mathscr{F}_G) = \left\{ \begin{array}{c} H \in \mathscr{X}_r : \textit{there exists } L \in \mathscr{X}_r \textit{ and } \varphi \in \mathfrak{G} \textit{ with} \\ H \leqslant L \textit{ and } \varphi(\mathscr{P}) \subset L \subset \varphi(\mathscr{P}_1) \end{array} \right\}.$$

Proof. — If $L \in \mathscr{X}_r$ and $\varphi \in \mathfrak{G}$ with $\varphi(\mathscr{P}) \subset L$ then φ defines an isomorphism between a finite coclass r quotient of $\mathscr{U}_r/\mathscr{P}$ and $\mathscr{U}_r/L$. The quotient of $\mathscr{U}_r/\mathscr{P}$ maps onto P_1 since $L \subset \varphi(\mathscr{P}_1)$. But such finite coclass r quotients of $\mathscr{U}_r/\mathscr{P}$ are precisely the groups P_n. Hence the coclass r p-group corresponding to $\mathscr{U}_r/H$ is a descendant of P_n. Conversely any coclass r p-group $\mathscr{U}_r/H$ which is in the family $\mathscr{F}_G$ must have a quotient $\mathscr{U}_r/L$ which is isomorphic to $\mathscr{U}_r/\mathscr{P}_n$ for some n. As we have proved above, these isomorphisms lift to automorphisms of $\mathscr{U}_r$. Hence $H \in \mathscr{X}(\mathscr{F}_G)$. Note that the set $\mathscr{X}(\mathscr{F}_G)$ is closed under the action of $\mathfrak{G}$ so the number of times a descendant $\mathscr{U}_r/H$ gets counted is still given by $|\mathfrak{G} : \mathrm{Stab}_{\mathfrak{G}}(H)|$. □

Proof of Theorem 8.4. — As in the proof of Theorem 1.12 we split up our zeta function:

$$\sum_{H \in \mathscr{X}(\mathscr{F}_G)} |\mathscr{U}_r : H|^{-s} |\mathfrak{G} : \mathrm{Stab}_{\mathfrak{G}}(H)|^{-1} =$$

$$\sum_{\mathscr{N} \leqslant K \lhd \mathscr{U}_r} |\mathscr{U}_r : K|^{-s} \sum_{\mathfrak{G}_1 \leqslant \mathfrak{K} \leqslant \mathfrak{G}} |\mathfrak{G} : \mathfrak{K}|^{-1} \sum_{H \in \mathscr{X}(\mathscr{U}_r, K, \mathfrak{K}) \cap \mathscr{X}(\mathscr{F}_G)} |K : H|^{-s} |\mathfrak{K} : \mathrm{Stab}_{\mathfrak{G}}(H)|^{-1}.$$

Let

$$\mathscr{M}(\mathscr{F}_G) = \bigcup_{H \in \mathscr{X}(\mathscr{U}_r, K, \mathfrak{K}) \cap \mathscr{X}(\mathscr{F}_G)} M(H) \times N(H) \subset \mathscr{N}^{(d+n)} \times \mathfrak{G}_1^{(r+t)}.$$

Then

$$\sum_{H \in \mathscr{X}(\mathscr{U}_r, K, \mathfrak{K}) \cap \mathscr{X}(\mathscr{F}_G)} |K : H|^{-s} |\mathfrak{K} : \mathrm{Stab}_{\mathfrak{G}}(H)|^{-1} = cc' \int_{\mathscr{M}(\mathscr{F}_G)} F(\mathbf{g}) F'(\mathbf{x}) d\mu d\nu.$$

So to prove rationality of this integral we just have to prove that $\mathscr{M}(\mathscr{F}_G)$ is a definable subset. Since

$$\mathscr{M}(\mathscr{F}_G) = \left\{ \begin{array}{l} (\mathbf{h}, \mathbf{t}, \mathbf{u}, \mathbf{s}) \in \mathscr{M}_r(K, \mathfrak{K}) : (\mathbf{h}, \mathbf{t}) \text{ is a basis for a subgroup H satisfying} \\ \text{"there exists } L \in \mathscr{X}_r \text{ and } \varphi \in \mathfrak{G} \text{ with } H \leqslant L \text{ and } \varphi(\mathscr{P}) \subset L \subset \varphi(\mathscr{P}_1)" \end{array} \right\}$$

we have to prove that this last statement "there exists $L \in \mathscr{X}_r$ and $\varphi \in \mathfrak{G}$ with $H \leqslant L$ and $\varphi(\mathscr{P}) \subset L \subset \varphi(\mathscr{P}_1)$" is definable. We can quantify over subgroups L with $H \leqslant L \in \mathscr{X}_r$ by quantifying over bases for such subgroups. Also the concept of a basis makes sense for subgroups like $\mathscr{P}$ which are not open in $\mathscr{U}_r$. We therefore fix such a basis and also a basis for $\mathscr{P}_1$. We can also quantify over elements of $\mathfrak{G}$ since they are given by expressions of the form uv_i for $i = 1, ..., s$. So it becomes a definable statement to test whether $\varphi(\mathscr{P}) \subset L \subset \varphi(\mathscr{P}_1)$. Hence the whole condition "there exists $L \in \mathscr{X}_r$ and $\varphi \in \mathfrak{G}$ with $H \leqslant L$ and $\varphi(\mathscr{P}) \subset L \subset \varphi(\mathscr{P}_1)$" is definable and consequently so is the subset $\mathscr{M}(\mathscr{F}_G)$. By [4] and [8] this implies then that $\zeta_{\mathscr{F}_G}(s)$ is a rational function in p^{-s} and completes the proof of Theorem 8.4. □

Proof of Theorem 8.6. — Fix a twig type $\mathfrak{t} \in \mathfrak{T}(M, N(\mathscr{F}_G))$. Suppose that $\mathscr{U}_r/H \cong P_n$, one of the mainline groups. We define the *descendant twig* $\mathfrak{t}_H(M)$ of H of length M, by

(1) the nodes of $\mathfrak{t}_H(M)$ are equivalence classes of subgroups $L \in \mathscr{X}_r$ of H of index at most p^M in H with the property that L does not contain any other subgroup H_1 with $\mathscr{U}_r/H_1 \cong P_{n+k}$ and $k > 0$;

(2) there is an edge connecting nodes of $\mathfrak{t}_H(M)$ corresponding to L_1 and L_2 if $L_1 \subset L_2$ and L_1 has index p in L_2.

To prove the rationality of $\zeta_{\mathscr{F}_G, M, \mathfrak{t}}(s)$ we have to prove that the following statement is definable:

> "$(\mathbf{h}, \mathbf{t})$ is a basis for a subgroup H such that there exist $\varphi \in \mathfrak{G}$ and $n \in \mathbf{N}$ with $\varphi(\mathscr{P}_n) = H$ and $\mathfrak{t}_H(M) = \mathfrak{t}$".

The statement "there exist $\varphi \in \mathfrak{G}$ and $n \in \mathbf{N}$ with $\varphi(\mathscr{P}_n) = H$" is equivalent to

(1) "there exist $\varphi \in \mathfrak{G}$ and $R \in \mathscr{X}_r$ with $\mathscr{P} \subset R \subset \mathscr{P}_1$ and $\varphi(R) = H$"

which is definable.

We can define when a group $L \in \mathscr{X}_r$ is part of the descendant twig $\mathfrak{t}_H(M)$ of length M of the group H. This involves the following statements:

(a) "for some $m \leqslant M$ there exists a chain of subgroups

$$H = L_0 \gneqq L_1 \gneqq \ldots \gneqq L_{m-1} \gneqq L_m = L$$

such that if $L_j \geqslant K \geqslant L_{j+1}$ then $K = L_j$ or L_{j+1}"; and

(b) "if there exists $R_1 \in \mathscr{K}_r$ with $\mathscr{P} \subset R_1 \subset \mathscr{P}_1$ and $L \subset \varphi(R_1)$ then $R_1 \subset R$ implies that $R_1 = R$".

Condition (a) ensures that we are only counting groups of length at most M from H. In (b), φ and R are the automorphism and group defined in condition (1). Condition (b) says that $\mathscr{U}_r/L$ is not a descendant of any mainline group below P_n.

Let $\mathfrak{N}_i$ be the finite set of nodes of $\mathfrak{t}$ of length i from the root of $\mathfrak{t}$ and $1 + e_{i1}, \ldots, 1 + e_{iq_i}$ be the valencies of these nodes for $i = 0, \ldots, M - 1$. The nodes of distance M from the root have valency 1. Then to ensure that $\mathfrak{t}_H(M) = \mathfrak{t}$ we want to say that for each H satisfying (1) there exist subgroups L_{ij} $(1 \leqslant i \leqslant M,\ 1 \leqslant j \leqslant q_i)$ such that (putting $L_{01} = H$):

(i) L_{ij} satisfy conditions (a) and (b);

(ii) $L_{i+1,l}$ is a maximal subgroup of L_{ij} for $e_{i1} + \cdots + e_{i,j-1} < l \leqslant e_{i1} + \cdots + e_{ij}$;

(iii) for $j \neq l$ there does not exist $\alpha \in \mathfrak{G}$ such that $L_{ij}^{\alpha} = L_{il}$;

(iv) if L is a group satisfying (a) and (b) then there exists $\alpha \in \mathfrak{G}$ such that $L^{\alpha} = L_{mj}$ for some j.

This constitutes a finite number of definable statements.

Hence we can definably describe those subgroups H which define mainline groups with twigs of type $\mathfrak{t}$. Hence by [4] and [8] $\zeta_{\mathscr{F}_G, M, \mathfrak{t}}(s)$ is a rational function. This competes the proof of Theorem 8.6. □

As a corollary we have therefore proved our periodicity result Theorem 8.3.

Note that it was important to bound the length of twigs we are considering if we are going to have a chance of making a definable statement. It may be possible though to exploit these ideas further to understand the sort of periodicity down the twigs that is conjectured by Newman for example in the tree of coclass 1 5-groups [31]. For example, we can use a similar argument to prove the rationality of the zeta function

$$\sum_{\mathfrak{t}_P(M) = \mathfrak{t}} |P|^{-s}$$

where P ranges over all points in the tree $\mathscr{F}_G$ (rather than just mainline groups) and $\mathfrak{t}_P(M)$ is the descendant twig of all non-mainline groups of distance at most M from P. We can also define terminal points in the tree and capture the rationality of a zeta function counting cuttings of length M containing a terminal point in the tree.

Our approach does not offer yet any contribution to the quantitative side of the Periodicity Conjecture P of Newman and O'Brien. Although the definability of the integrals looks rather unpromising to be able to ascertain the precise period, it is possible that a more direct analysis of the groups $\mathscr{U}_r$ for $p = 2$ might yield more precise information about the period. After all, $\mathscr{U}_r$ for $p = 2$ is a finite extension of

a free abelian pro-p group. In [18], the zeta functions counting normal subgroups in finite extensions of free abelian groups is considered and related to the work of Hey, Solomon, Bushnell and Reiner. It is possible then that this approach could yield information about the period. For example, the period or length of the recurrence relation is the degree of the denominator in these rational functions. The paper [18] seeks to understand what the effect of extending a free abelian group by a finite group has on the rational function. This would be relevant therefore to understanding the period of these trees.

To understand the zeta functions attached to $\mathcal{U}_r$ in this part we have used integrals that are definable in the language $\mathcal{L}_G$. These integrals translate into integrals definable in the analytic language $\mathcal{L}_{an}^{D}$ for the p-adic integers of [4]. Since $\mathcal{U}_r$ is a finite extension of a finitely generated nilpotent group, it is possible to use the analysis of [21] for finitely generated nilpotent groups together with the analysis of [8] for counting subgroups in finite extensions to write the parts of the integrals over bases for subgroups in $\mathcal{U}_r$ in the algebraic language for the p-adic integers first used in [3]. At present there doesn't seem a great advantage in this simpler language since its power comes in understanding uniformity questions across all primes. Such uniformity properties are not so expected in this setting since the values of $g(p, r)$ and $h(p, r)$ in the coclass conjectures depend on p. It would be interesting though to see whether a bound on the periods as we vary the primes could be obtained somehow from an analysis of these integrals.

9. Examples

9.1. *2-groups and 3-groups of coclass* 1

Let us begin with a description of the zeta functions $\zeta_{ccl}^{1,p}(s)$ of coclass 1 p-groups for $p=2$ and 3.

Theorem **9.1.** — (1)

$$\zeta_{ccl}^{1,2}(s)=\frac{2^{-2s}(2+2^{-2s})}{(1-2^{-s})}$$

(2)

$$\zeta_{ccl}^{1,3}(s)=\frac{3^{-2s}(2+2\cdot 3^{-s}+2\cdot 3^{-2s}+4\cdot 3^{-3s}+3\cdot 3^{-4s})}{(1-3^{-2s})}$$

Proof. — (1) For $p=2$, $c(1,2,2)=c(1,3,2)=2$, and $c(1,n,2)=3$ for $n \geqslant 4$. This is classical.

(2) For $p=3$, $c(1,2,3)=c(1,3,3)=2$, $c(1,4,3)=4$ and $c(1,2n-1,3)=6$ whilst $c(1,2n,3)=7$ for $n \geqslant 3$. These numbers were determined by N. Blackburn in [1]. □

Note that the tree for coclass 1 3-groups actually has bounded twig lengths, unlike our next example where the twig lengths are unbounded.

9.2. *5-groups of coclass* 1

In [31], Newman gives a conjectural description of the tree $\mathscr{K}_5$ of 5-groups of coclass 1. It is known that it consists of a single unbounded path made out of (non-cyclic) finite quotients of the central quotient of the wreath product of the additive group of the 5-adic integers by a cyclic group of order 5. Each quotient of order 5^m we denote by U_m. It is coclass settled by 5^6. Also every group in $\mathscr{K}_5$ of order 5^n has a quotient U_m with $2m \geqslant n$. Thus every path beginning at U_m and not passing through U_{m+1} has length at most m.

Newman has calculated $c(1,n,5)$ for $n \leqslant 30$. This revealed minor irregularities for $n \leqslant 16$. But the descendant tree of U_9, which we denote by $\mathscr{K}_5(9)$, revealed a possible doubly periodic pattern which is described in Table 4(m) of [31]. Using this conjectural description we can give the following conjectural description of the zeta function of the tree $\mathscr{K}_5(9)$.

Theorem **9.2.** — *Define*

$$\zeta_{\mathscr{K}_5(9)}(s) = \sum_{P \in \mathscr{K}_5(9)} |P|^{-s} = \sum_{n=9}^{\infty} a_n(\mathscr{K}_5(9))5^{-ns}.$$

If Newman's description of the tree $\mathscr{K}_5(9)$ *is correct then*

(1)

$$\zeta_{\mathscr{K}_5(9)}(s) = \frac{P(5^{-s})}{(1-5^{-8s})^2}$$

where

$$P(x) = x^9 + 18x^{10} + 38x^{11} + 106x^{12} + 163x^{13} + 201x^{14} + 393x^{15} + 582x^{16} + 762x^{17} + 939x^{18} + 955x^{19} + 1115x^{20} + 1134x^{21} + 1325x^{22} + 1327x^{23} + 1499x^{24}$$

(2) $a_n = a_n(\mathscr{H}_5(9))$ *satisfies the following linear recurrence relation for* $n \geqslant 25$:

$$a_{n+16} = 2a_{n+8} - a_n \ ;$$

the initial conditions are provided by the polynomial $\mathrm{P}(x)$.

Since Newman has calculated $c(1, n, 5)$ for $n \leqslant 30$ we know already the finite polynomial $\zeta_{\mathrm{ccl}}^{1,5}(s) - \zeta_{\mathscr{H}_5(9)}(s)$ in 5^{-s}. Hence we can get a conjectural description of $\zeta_{\mathrm{ccl}}^{1,5}(s)$. We omit this description since the tyranny of the small (i.e. the minor irregularities for $n \leqslant 16$) results in rather a large numerator.

Corollary **9.3.** — *If Newman's description is correct then there exists a polynomial* $\mathrm{P}_1(x)$ *of degree 24 such that*

$$\zeta_{\mathrm{ccl}}^{1,5}(s) = \frac{\mathrm{P}_1(5^{-s})}{(1-5^{-8s})^2}.$$

9.3. *2-groups of coclass 2*

In [32] some description is given of the 2-groups of coclass 2. In particular there are 29 groups of order 2^{2n-1} and 38 groups of order 2^{2n} for $n \geqslant 4$. Hence we have

Theorem **9.4.** — *There exists a polynomial* $\mathrm{Q}(x)$ *of degree 8 (which again captures the tyranny of the small) such that*

$$\zeta_{\mathrm{ccl}}^{2,2}(s) = \frac{\mathrm{Q}(2^{-s})}{(1-2^{-2s})}.$$

REFERENCES

[1] N. Blackburn, On a special class of p-groups, *Acta Math.* **100** (1958), 49-92.

[2] R. M. Bryant and J. R. J. Groves, Algebraic groups of automorphisms of nilpotent groups and Lie algebras, *J. London Math. Soc.* **33** (1986), 453-466.

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

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

[5] J. Denef and F. Loeser, Motivic Igusa zeta functions, *J. Algebraic Geom.*, **7** (1998), 505-537.

[6] J. Denef and F. Loeser, Germs of arcs on singular algebraic varieties and motivic integration, *Invent. Math.*, **135** (1999), 201-232.

[7] J. D. DIXON, M. P. F. du SAUTOY, A. MANN and D. SEGAL, Analytic pro-p groups, Second Edition, *Cambridge Studies in Advanced Mathematics*, **61**, Cambridge, CUP, 1999.

[8] M. P. F. du SAUTOY, Finitely generated groups, p-adic analytic groups and Poincaré series, *Annals of Math.* **137** (1993), 639-670.

[9] M. P. F. du SAUTOY, Zeta functions and counting finite p-groups, *Electronic Research Announcements of the American Math. Soc.*, **5** (1999), 112-122.

[10] M. P. F. du SAUTOY, A nilpotent group and its elliptic curve: non-uniformity of local zeta functions of groups, MPI preprint 2000-85. To appear in *Israel J. of Math.* **126**.

[11] M. P. F. du SAUTOY, Counting subgroups in nilpotent groups and points on elliptic curves, MPI preprint 2000-86.

[12] M. P. F. du SAUTOY, Natural boundaries for zeta functions of groups, preprint.

[13] M. P. F. du SAUTOY and F. J. GRUNEWALD, Analytic properties of Euler products of Igusa-type zeta functions and subgroup growth of nilpotent groups, *C. R. Acad. Sci. Paris* **329**, Série 1 (1999), 351-356.

[14] M. P. F. du SAUTOY and F. J. GRUNEWALD, Analytic properties of zeta functions and subgroup growth, *Annals of Math.* **152** (2000), 793-833.

[15] M. P. F. du SAUTOY and F. J. GRUNEWALD, Uniformity for 2-generator free nilpotent groups, in preparation.

[16] M. P. F. du SAUTOY and F. LOESER, Motivic zeta functions of infinite dimensional Lie algebras, École polytechnique, preprint series 2000-12.

[17] M. P. F. du SAUTOY and A. LUBOTZKY, Functional equations and uniformity for local zeta functions of nilpotent groups, *Amer. J. Math.* **118** (1996), 39-90.

[18] M. P. F. du SAUTOY, J. J. MCDERMOTT and G. C. SMITH, Zeta functions of crystallographic groups and analytic continuation, *Proc. London Math. Soc.* **79** (1999), 511-534.

[19] M. P. F. du SAUTOY and D. SEGAL, Zeta functions of groups, in *New horizons in pro-p groups. Progress in Mathematics*, vol. **184** (ed M. P. F. du Sautoy, D. Segal and A. Shalev), p. 249-286. Boston, Birkhäuser (2000).

[20] M. D. FRIED and M. JARDEN, *Field Arithmetic*, Springer-Verlag, Berlin, Heidelberg, New York, 1986.

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

[22] G. HIGMAN, Enumerating p-groups, I, *Proc. London Math. Soc.* **10** (1960), 24-30.

[23] G. HIGMAN, Enumerating p-groups, II, *Proc. London Math. Soc.* **10** (1960), 566-582.

[24] K. IRELAND and M. ROSEN, A classical introduction to modern number theory, Second Edition, *Graduate texts in mathematics* **84**, Springer-Verlag, New York, Berlin, Heidelberg, 1993.

[25] S. LANG, *Algebra*, Addison-Wesley, Reading, MA, 1965.

[26] C. R. LEEDHAM-GREEN and S. MCKAY, On p-groups of maximal class II, *Quart. J. Math. Oxford* (2) **29** (1978), 175-186.

[27] C. R. LEEDHAM-GREEN and S. MCKAY, On p-groups of maximal class III, *Quart. J. Math. Oxford* (2) **29** (1978), 281-299.

[28] C. R. LEEDHAM-GREEN and M. F. NEWMAN, Space groups and groups of prime-power order I, *Arch. Math.* (Basel) **35** (1980), 193-202.

[29] C. R. LEEDHAM-GREEN, The structure of finite p-groups, *J. London Math. Soc.* **50** (1994), 49-67.

[30] W. MAGNUS, A. KARRAS and D. SOLITAR, *Combinatorial Group Theory*, Wiley, Chichester, UK, 1966.

[31] M. F. NEWMAN, Groups of prime-power order, Groups-Canberra 1989, *Lecture Notes in Math.*, **1456** Springer-Verlag (1990), 49-62.

[32] M. F. NEWMAN and E. A. O'BRIEN, Classifying 2-groups by coclass, *Trans. Amer. Math. Soc.* **351** (1999), 131-169.

[33] V. P. PLATONOV, The problem of strong approximation and the Kneser-Tits conjecture for algebraic groups, *Math. USSR-Izv.* **3** (1969), 1139-1147.

[34] V. P. PLATONOV, Addendum, *Math. USSR-Izv.* **4** (1970), 784-786.

[35] V. P. PLATONOV and A. S. RAPINCHUK, *Algebraic Groups and Number Theory, Pure and Applied Mathematics* **139**, London, Academic Press, 1994.

[36] D. SEGAL, Polycyclic Groups, *Cambridge tracts in mathematics*, **82**, CUP (1983).

[37] A. SHALEV, The structure of finite p-groups: effective proof of the coclass conjectures, *Invent. Math.* **115** (1994), 315-345.

[38] C. C. SIMS, Enumerating p-groups, *Proc. London Math. Soc.* **15** (1965), 151-166.

[39] R. P. STANLEY, Enumerative Combinatorics, vol. 1, *Cambridge Studies in Advanced Mathematics*, **49**, CUP, 1997.

M. du S.
DPMMS, Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 0WB, UK
dusautoy@dpmms.cam.ac.uk
http://www.dpmms.cam.ac.uk/~dusautoy

current address:
Mathematical Institute
24-29 St. Giles
Oxford 0X13LB, UK
dusautoy@maths.ox.ac.uk

Manuscrit reçu le 11 décembre 2000.