Available online at www.sciencedirect.com
ScienceDirect
C. R. Acad. Sci. Paris, Ser. I 347 (2009) 1347–1350
COMPTES RENDUS MATHEMATIQUE

Group Theory

Enumerating finite class-2-nilpotent groups on 2 generators

Christopher Voll

School of Mathematics, University of Southampton, University Road, Southampton SO17 1BJ, UK

Received 10 August 2009; accepted after revision 27 October 2009

Presented by Jean-Pierre Serre

Abstract

We compute the numbers $g(n, 2, 2)$ of nilpotent groups of order n, of class at most 2 generated by at most 2 generators, by giving an explicit formula for the Dirichlet generating function $\sum_{n=1}^{\infty} g(n, 2, 2)n^{-s}$. ***To cite this article: C. Voll, C. R. Acad. Sci. Paris, Ser. I 347 (2009).***

Résumé

Énumération des groupes nilpotents de classe 2 engendrés par 2 générateurs. On calcule les nombres $g(n, 2, 2)$ de groupes nilpotents d'ordre n, de classe au plus 2, engendrés par au plus 2 générateurs, en donnant une formule explicite pour la fonction génératrice de Dirichlet $\sum_{n=1}^{\infty} g(n, 2, 2)n^{-s}$. ***Pour citer cet article : C. Voll, C. R. Acad. Sci. Paris, Ser. I 347 (2009).***

1. Introduction and statement of results

In [1], du Sautoy shows how G. Higman's PORC-conjecture on the numbers $f(n, p)$ of isomorphism types of p-groups of order p^n can be studied using various Dirichlet generating functions (or zeta functions) associated with groups. Higman conjectured that the numbers $f(n, p)$ should be 'polynomial on residue classes', i.e. that for all n there should exist an integer $N = N(n)$ and polynomials $f_1(X), \dots, f_N(X) \in \mathbb{Z}[X]$ such that $f(n, p) = f_i(p)$ if $p \equiv i$ modulo N. For positive integers c and d, we define $\mathcal{N}(c, d)$ to be the set of finite nilpotent groups (up to isomorphism) of class at most c generated by at most d generators, and put

$$g(n, c, d) := \#\{G \in \mathcal{N}(c, d) \mid |G| = n\}.$$

We define the Dirichlet generating function

$$\zeta_{c,d}(s) := \sum_{n=1}^{\infty} g(n, c, d)n^{-s},$$

where s is a complex variable. In [1, Theorem 1.5] du Sautoy shows that

E-mail address: C.Voll.98@cantab.net.

1631-073X/$ – see front matter
doi:10.1016/j.crma.2009.10.024

$$\zeta_{c,d}(s) = \prod_{p\,\text{prime}} \zeta_{c,d,p}(s), \tag{1}$$

where, for a prime p,

$$\zeta_{c,d,p}(s) := \sum_{i=0}^{\infty} g\big(p^i, c, d\big) p^{-is}.$$

This 'Euler product' reflects the fact that finite nilpotent groups are the direct products of their Sylow p-subgroups. Du Sautoy goes on to prove that, for all primes p, the function $\zeta_{c,d,p}(s)$ is rational in p^{-s} [1, Theorem 1.6]. In the remainder of [1, Part I] he shows that these local zeta functions are amenable to methods from model theory and algebraic geometry, and explains how in this setup Higman's conjecture translates into a question about the reduction modulo p of various ($\mathbb{Z}$-defined) algebraic varieties.

Almost none of the functions $\zeta_{c,d}(s)$ have been explicitly calculated so far. For $c = 1$, it is a trivial and well-known consequence of the structure theorem for finitely generated abelian groups that, for all $d \in \mathbb{N}$,

$$\zeta_{1,d}(s) = \prod_{i=1}^{d} \zeta(is),$$

where $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ is the Riemann zeta function [1, p. 65]. The purpose of the current note is to give a formula for the generating function $\zeta_{2,2}(s)$. This seems to be the only one among the functions $\zeta_{c,d}(s)$, $c > 1$, for which explicit computations exist (see also [1, Problem 4]).

Theorem 1.1. *For* $(c, d) = (2, 2)$ *we have*

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

Corollary 1.2. *For all primes p, we have*

$$\zeta_{2,2,p}(s) = 1 + t + 2t^2 + 4t^3 + 6t^4 + 8t^5 + 13t^6 + 17t^7 + 23t^8 + 31t^9 + 40t^{10} + 50t^{11} + 65t^{12} + O\big(t^{13}\big)$$

(*where* $t = p^{-s}$). *The abscissa of convergence of* $\zeta_{2,2}(s)$ *is* $\alpha = 1$, *and* $\zeta_{2,2}(s)$ *has an analytic continuation to the whole complex plane. This continued function has a simple pole at* $s = 1$, *and thus*

$$\sum_{m=1}^{n} g(m, 2, 2) \sim \frac{\pi^6}{540}\zeta(3)^2 n = 2.5725\ldots n.$$

(*Here* $f(n) \sim g(n)$ *means that* $\lim_{n\to\infty} f(n)/g(n) = 1$.)

We note that — as in the case $c = 1$ — the local functions $\zeta_{2,2,p}(s)$ are rational in p^{-s} with *constant* coefficients (as the prime p varies). We expect this 'strong uniformity' in the prime p to be the exception rather than the rule. Indeed, computer calculations of $g(p^i, 2, 3)$ for $p \in \{2, 3, 5\}$ and small values of i show that these numbers do depend on the prime.[1] A 'restricted' analogue of Higman's PORC-conjecture would ask whether, for each pair (c, d), the coefficients of the functions $\zeta_{c,d,p}(s)$ as rational functions in p^{-s} are polynomial in p on residue classes of p modulo $N = N(c, d)$. We note that it is well known [2, Theorem 2] that, for all $d \geqslant 2$ and all primes p, the local zeta functions $\zeta^{\triangleleft}_{F_{2,d},p}(s)$ enumerating normal subgroups of finite p-power index in the free nilpotent groups $F_{2,d}$ are rational functions in p and p^{-s} (see also [5]). We refer to [1] for an explanation of a link between these Dirichlet generating functions and the functions $\zeta_{2,d}(s)$ defined above.

In our proof of Theorem 1.1 we adopt the strategy outlined in [1, Section 2]. It proceeds by finding 'normal form'-representatives of certain double cosets of integral matrices, and avoids any algebro-geometric or model-theoretic considerations. We do, however, use methods pioneered in [2].

1 We thank Eamonn O'Brien for pointing this out to us.

2. Proof of Theorem 1.1

The 'Euler product decomposition' (1) above reduces the problem to the enumeration of (isomorphism classes of) p-groups of class at most 2 generated by at most 2 generators, for a fixed prime p. Each of these groups occurs as the quotient of the group $\widehat{F}_p$, the pro-p-completion of the free nilpotent group $F := F_{2,2}$ of class 2 on 2 generators, by a normal subgroup N of finite index. The automorphism group $\mathfrak{G}_p$ of $\widehat{F}_p$ acts on the lattice of these normal subgroups, and it is known that two subgroups give rise to the same (isomorphism type of) quotient if and only if they are equivalent to each other under this action [1, Proposition 2.5]. To summarize, we have that, for all primes p,

$$\zeta_{2,2,p}(s) = \sum_{N \lhd \widehat{F}_p} |\widehat{F}_p : N|^{-s} \big|\mathfrak{G}_p : \mathrm{Stab}_{\mathfrak{G}_p}(N)\big|^{-1}$$

(cf. [1, Theorem 1.13]). To turn this into an explicit formula for $\zeta_{2,2,p}(s)$, we firstly linearize the problem of counting normal subgroups in the group $\widehat{F}_p$ up to the action of $\mathfrak{G}_p$, in the following way. Consider the 'Heisenberg Lie ring' $L := L_{2,2} := F/Z(F) \oplus Z(F)$ associated with F, with Lie bracket induced from taking commutators in F. It is well known [2, Remark on p. 206] that normal subgroups of index p^n in $\widehat{F}_p$ correspond to ideals of index p^n in the $\mathbb{Z}_p$-Lie algebra $L_p := L \otimes \mathbb{Z}_p$, and it is easily verified that orbits under $\mathfrak{G}_p$ in the lattice of normal subgroups of $\widehat{F}_p$ correspond to orbits under $\mathrm{Aut}(L_p)$. Having chosen a basis for L, e.g. (x, y, z) with $[x, y] = z$, full sublattices Λ in $(L_p, +)$ may be identified with cosets ΓM, $\Gamma := \mathrm{GL}_3(\mathbb{Z}_p)$, $M \in \mathrm{Mat}(3, \mathbb{Z}_p) \cap \mathrm{GL}_3(\mathbb{Q}_p)$, by encoding in the rows of M the coordinates (with respect to the chosen basis, viewed as a basis for the $\mathbb{Z}_p$-Lie algebra L_p) of generators for Λ.

Given the basis (x, y, z) as above, every coset ΓM corresponding to a lattice of finite index in L_p contains a unique matrix of the form

$$M = \begin{pmatrix} p^{n_1} & a_{12} & a_{13} \\ & p^{n_2} & a_{23} \\ & & p^{n_3} \end{pmatrix}, \tag{2}$$

with $n_1, n_2, n_3 \in \mathbb{N}_0 := \{0, 1, 2, \ldots\}$, $0 \leqslant a_{12} < p^{n_2}$ and $0 \leqslant a_{13}, a_{23} < p^{n_3}$. It is easy to see and well known that ΓM corresponds to an *ideal* in L_p (of index $p^{n_1+n_2+n_3}$) if and only if

$$n_3 \leqslant n_2, n_1, v_p(a_{12}) \tag{3}$$

(where v_p denotes the p-adic valuation).

The choice of basis allows us to identify $\mathrm{Aut}(L_p)$ with the group of matrices of the form

$$\left\{ \begin{pmatrix} \alpha & * \\ & \det(\alpha) \end{pmatrix} \,\middle|\, \alpha \in \mathrm{GL}_2(\mathbb{Z}_p) \right\} \subseteq \Gamma.$$

The action of $\mathrm{Aut}(L_p)$ on the lattice of ideals of finite index in L_p is then simply given by the natural (right-)action on the set of cosets ΓM. We claim that the matrices of the form (2) with

$$n_1 = e_1 + e_2 + e_3, \qquad n_2 = e_2 + e_3, \qquad n_3 = e_3, \qquad a_{12} = 0, \qquad a_{13} = p^{e_4}, \qquad a_{23} = p^{e_5}, \tag{4}$$

where

$$e_1, \ldots, e_5 \in \mathbb{N}_0, \qquad e_4, e_5 \leqslant e_3, \qquad e_5 \leqslant e_4 \leqslant e_5 + e_1 \tag{5}$$

form a complete set of representatives of the double cosets

$$\Gamma \backslash \big(\mathrm{Mat}(3, \mathbb{Z}_p) \cap \mathrm{GL}_3(\mathbb{Q}_p)\big) / \mathrm{Aut}(L_p).$$

This suffices as then

$$\zeta_{2,2,p}(s) = \sum_{\Gamma \backslash M / \mathrm{Aut}(L_p)} \big|\det(M)\big|^{-s} = \sum_{(e_1,\ldots,e_5) \in \mathbb{N}_0^5 \text{ satisfying (5)}} p^{-3e_3 s - 2e_2 s - e_1 s}$$
$$= \frac{1}{(1-p^{-s})(1-p^{-2s})(1-p^{-3s})^2(1-p^{-4s})} = \zeta_p(s)\zeta_p(2s)\zeta_p(3s)^2\zeta_p(4s),$$

as an easy calculation yields.

To prove our claim, it suffices to show that every double coset contains a matrix of the form (2), satisfying (4) and (5), and that, if N and N' are in this normal form, the double cosets defined by them coincide only if $N = N'$.

We start by observing that every double coset of matrices of the form (2) satisfying the 'ideal condition' (3) contains a matrix of the form (2) with

$$n_1 = e_1 + e_2 + e_3, \qquad n_2 = e_2 + e_3, \qquad n_3 = e_3, \qquad a_{12} = 0,$$

where

$$e_1, e_2, e_3 \in \mathbb{N}_0, \qquad e_4 := v_p(a_{13}) \leqslant e_3, \qquad e_5 := v_p(a_{23}) \leqslant e_3.$$

This is because $\mathrm{Aut}(L_p)$ contains a copy of $\mathrm{GL}_2(\mathbb{Z}_p)$, allowing us to bring the top-left 2×2-block of N into 'Smith normal form'. By a suitable base change we may also arrange for $a_{13} = p^{e_4}, a_{23} = p^{e_5}$. Furthermore we can achieve that $e_5 \leqslant e_4 \leqslant e_5 + e_1$ as we can always add multiples of the first row to the second row and multiples of p^{e_1} times the first row to the second row, each time 'clearing' the a_{21}- and a_{12}-entry respectively by right-multiplication by suitable elements in $\mathrm{Aut}(L_p)$, namely elementary column operations involving only the first two columns, leaving the third column stable.

Now assume that we are given matrices N and N' in normal form (2), satisfying (4) and (5), with associated invariants $(e_1, \ldots, e_5)$ and $(e'_1, \ldots, e'_5)$, respectively. For N and N' to define the same double cosets it is clearly necessary that $(e_1, e_2, e_3) = (e'_1, e'_2, e'_3)$. Also, necessarily $e_5 = e'_5$, as e_5 determines the p-adic norm of the last column of N, which is invariant both by left-multiplication by elements in Γ and by right-multiplication by $\mathrm{Aut}(L_p)$. We thus have, without loss of generality,

$$N = \begin{pmatrix} p^{e_1+e_2+e_3} & & p^{e_5+m+n} \\ & p^{e_2+e_3} & p^{e_5} \\ & & p^{e_3} \end{pmatrix}, \qquad N' = \begin{pmatrix} p^{e_1+e_2+e_3} & & p^{e_5+m} \\ & p^{e_2+e_3} & p^{e_5} \\ & & p^{e_3} \end{pmatrix},$$

where $m, n \geqslant 0, m + n \leqslant e_3$ and therefore in particular $m < e_3$. If N and N' were to define the same double coset, we must be able to 'adjust' the a_{13}-entry of N to have valuation p^{e_5+m} by a suitable row operation. The only way to achieve this is to add up^m times the second row to the first, where u is a p-adic unit. If $m > 0$, there is no other way to achieve Smith normal form on the top-left 2×2-block than to reverse this row operation. If $m = 0$ the only alternative is to choose the a_{12}-entry as a pivot to obtain this, which again has the invariants of N, not of N' if $n \neq 0$. Thus $n = 0$, completing the proof of Theorem 1.1.

Acknowledgements

The result presented in this note forms part of my Cambridge Ph.D. thesis [4], which was supervised by Marcus du Sautoy and partly funded by the Studienstiftung des deutschen Volkes and the Cambridge European Trust. I would like to thank Eamonn O'Brien for providing me with various computer-generated numerical data, which proved immensely helpful. These computations are based on [3].

References

[1] M.P.F. du Sautoy, Counting p-groups and nilpotent groups, Publ. Math. I.H.E.S. 92 (2000) 63–112.
[2] F.J. Grunewald, D. Segal, G.C. Smith, Subgroups of finite index in nilpotent groups, Invent. Math. 93 (1988) 185–223.
[3] E.A. O'Brien, The p-group generation algorithm, J. Symbolic Comput. 9 (5–6) (1990) 677–698 (Computational group theory, Part 1).
[4] C. Voll, Zeta functions of groups and enumeration in Bruhat–Tits buildings, Ph.D. thesis, University of Cambridge, 2002.
[5] C. Voll, Normal subgroup growth in free class-2-nilpotent groups, Math. Ann. 332 (2005) 67–79.