ISRAEL JOURNAL OF MATHEMATICS, Vol. 68, No. 1, 1989

COUNTING FINITE INDEX SUBGROUPS AND THE P. HALL ENUMERATION PRINCIPLE

BY

ISHAI ILANI

Department of Mathematics, The Hebrew University of Jerusalem, Jerusalem 91904, Israel

ABSTRACT

We apply the P. Hall enumeration principle to count the number of subgroups of a given index in the free pro-p group and the free abelian group. We shall present an infinite family of non-isomorphic pro-p groups with the same zeta function.

1. Introduction

Let G be a finitely generated group; let $a_n = a_n(G)$ be the number of subgroups of G of index n. In recent years there has been some interest in the function $G \rightarrow \{a_n(G)\}_{n=1}^{\infty}$ (see [H], [GSS], [S], [J] and the references therein). In this paper we show how the P. Hall enumeration principle can be applied to the study of this function for various groups.

M. Hall ([H]) gave a recursive formula for $a_n(F_r)$, where F_r is the free group on r generators. The same formula holds also for the free pro-finite group $\hat{F}_r$, by the one-to-one correspondence between its finite index (open) subgroups and those of F_r.

In this note we give a recursive formula for $a_n(\widehat{F_r(p)})$, where $\widehat{F_r(p)}$ denotes the free pro-p group on r generators.

We should mention that the subgroups of index p^n in $\widehat{F_r(p)}$ are not in one-to-one correspondence with those of index p^n in F_r. Rather they correspond to the subnormal subgroups of F_r of that index, so our formula counts also these subgroups of F_r.

Received May 31, 1988 and in revised form July 11, 1989

One way to encode the numbers $a_n(G)$ is by introducing the Dirichlet series:

$$f_G(s) = \sum_{n=1}^{\infty} a_n(G) n^{-s} = \sum_{n=1}^{\infty} a_n n^{-s} \qquad \text{(see [GSS]).}$$

For $G = \mathbf{Z}$, $f_G(s)$ is the classical Riemann zeta function, and so in general $f_G(s)$ is called the zeta function of G. The zeta function of $\mathbf{Z}^r$ was computed by [BR] and [GSS]. We will show how P. Hall's principle can be applied to give a different proof after factoring $f_{\mathbf{Z}^r}(s)$ into its Euler product decomposition.

Another application of P. Hall's enumeration principle to our topic is a sufficient condition for two pro-p groups to have the same zeta function. We shall use this condition to present an infinite family of non-isomorphic pro-p groups with the same zeta function. This condition will also be used to give another proof of the following result (proved in [L]):

If a pro-p group G is $f(p^n)$-indexed with $f(p^n) = p^n(r-1)+1$ (i.e. $(G:K) = p^n$ implies $\operatorname{rk}(K) = p^n(r-1)+1$), then $G = \widehat{F_r(p)}$.

2. The P. Hall enumeration principle

Let C_p^r be an elementary abelian group of order p^r. Denote

$$\begin{bmatrix} r \\ t \end{bmatrix} = a_{p^t}(C_p^r) \qquad 0 \leqq t \leqq r.$$

One can easily see (considering C_p^r as a vector space) that

$$\text{(1)} \qquad \begin{bmatrix} r \\ t \end{bmatrix} = \frac{(p^r-1)(p^{r-1}-1)\cdots(p^{r-t+1}-1)}{(p^t-1)(p^{t-1}-1)\cdots(p-1)}.$$

From (1) we can obtain

$$\text{(2)} \qquad \begin{bmatrix} r+1 \\ t \end{bmatrix} = \begin{bmatrix} r \\ t \end{bmatrix} + p^{r-t+1}\begin{bmatrix} r \\ t-1 \end{bmatrix},$$

and by induction on r

$$\text{(3)} \qquad \prod_{t=0}^{r-1}(x-p^t) = \sum_{t=0}^{r}(-1)^t p^{t(t-1)/2}\begin{bmatrix} r \\ t \end{bmatrix} x^{r-t}.$$

Using these identities P. Hall [H2] stated an enumeration principle for finite p groups, and we shall state here a slight variant.

THEOREM 1 (P. Hall) [H2]. *Let G be a group, and $\Phi \lhd G$ such that $G/\Phi \cong C_p^r$. For $0 \leqq t \leqq r$, $1 \leqq i \leqq \left[{r \atop t}\right]$, denote by $K_{t,i}$ the subgroups such that*

$$\Phi \leqq K_{t,i} \leqq G, \qquad (G : K_{t,i}) = p^t.$$

(Obviously $K_{0,1} = G$, $K_{r,1} = \Phi$.)

Let A be a finite collection of subgroups of G such that each $H \in A$ is contained in at least one of the $K_{1,i}$'s, $1 \leqq i \leqq \left[{r \atop 1}\right]$.

For $K_{t,i}$ denote

$$n(K_{t,i}) = \#\{H \in A \mid H \leqq K_{t,i}\}.$$

Then

$$\sum_{t=0}^{r} (-1)^t p^{t(t-1)/2} \sum_{i=1}^{\left[{r \atop t}\right]} n(K_{t,i}) = 0. \tag{4}$$

3. Recursion formula for $\widehat{F_r(p)}$

Let $\widehat{F_r(p)}$ denote the free pro-p group (p a prime number) on r generators and denote

$$(*) \qquad A(n, r) = \begin{cases} 0, & n < 0, \\ a_{p^n}(\widehat{F_r(p)}), & n \geqq 0. \end{cases}$$

PROPOSITION 2. *For $n \geqq 1$*

$$A(n, r) = \sum_{t=1}^{r} (-1)^{t+1} \begin{bmatrix} r \\ t \end{bmatrix} p^{t(t-1)/2} A(n - t, p^t(r-1) + 1). \tag{5}$$

PROOF. Let Φ be the Frattini subgroup of $\widehat{F_r(p)}$. Then $\widehat{F_r(p)}/\Phi \cong C_p^r$ and each proper subgroup of $\widehat{F_r(p)}$ is contained in one of the $K_{1,i}$'s and thus we can apply the P. Hall enumeration principle. Each $K_{t,i}$ is a free pro-p group on $p^t(r-1)+1$ generators (cf. [LV]) and thus contains $A(n-t, p^t(r-1)+1)$ subgroups of index p^n in $\widehat{F_r(p)}$. The number of $K_{t,i}$'s for a fixed t is $\left[{r \atop t}\right]$, and the rest is a simple consequence of the P. Hall enumeration principle.

A recursion formula which involves only the number of subgroups of lower index in the same group, $\widehat{F_r(p)}$, can be obtained by the following:

LEMMA 3. *Suppose the numbers $A(n, r)$ are given recursively by*

$$A(n, r) = \begin{cases} 0, & n < 0, \\ 1, & n = 0, \\ \sum_{t=1}^{n} b_t^r A(n - t, f^t(r)), & n = 1, 2, \dots, \end{cases}$$

where $f: N \to N$ *is any function* (N *denotes the natural numbers*) $f^t(r) = f(f^{t-1}(r))$ ($f^0(r) = r$), *and* b_t^r *are given numbers. Then*

$$A(n, r) = \sum_{t=1}^{n} b_t^{f^{n-t}(r)} A(n-t, r).$$

Proof. Let $B^i = (b_{k,j}^i)$, $i = 0, 1, \ldots$ be the infinite matrix defined by

$$\begin{cases} b_{1,j}^i = b_j^{f^i(r)}, \\ b_{j+1,j}^i = 1, \\ b_{k,j}^i = 0, \quad \text{otherwise.} \end{cases}$$

Define $A^i = (a_{k,j}^i)$ inductively by

$$A^1 = B^0, \qquad A^{i+1} = A^i B^i.$$

By induction on n it is easy to see that, for $i \geqq 0$,

$$A^n \begin{bmatrix} A(i, f^n(r)) \\ A(i-1, f^{n+1}(r)) \\ \vdots \end{bmatrix} = \begin{bmatrix} A(n+i, r) \\ A(n+i-1, f(r)) \\ \vdots \end{bmatrix}$$

thus

$$A^n \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ \vdots \end{bmatrix} = A^n \begin{bmatrix} A(0, f^n(r)) \\ A(-1, f^{n+1}(r)) \\ \vdots \\ \vdots \\ \end{bmatrix} = \begin{bmatrix} A(n, r) \\ A(n-1, f(r)) \\ A(n-2, f^2(r)) \\ \vdots \\ \vdots \end{bmatrix}$$

Hence

$$a_{1,1}^n = A(n, r).$$

Now

$$a_{1,j}^n = \begin{cases} b_j^{f^{n-1}(r)} a_{1,1}^{n-1} + a_{1,j+1}^{n-1}, & n > 1, \\ b_j^r, & n = 1, \end{cases}$$

thus

$$\begin{aligned} a^n_{1,1} &= b_1^{f^{n-1}(r)} a^{n-1}_{1,1} + a^{n-1}_{1,2} \\ &= b_1^{f^{n-1}(r)} a^{n-1}_{1,1} + b_2^{f^{n-2}(r)} a^{n-2}_{1,1} + a^{n-2}_{1,3} \\ &= \sum_{t=1}^{n-1} b_t^{f^{n-t}(r)} a^{n-t}_{1,1} + a^1_{1,n}. \end{aligned}$$

By substituting $A(n,r) = a^n_{1,1}$, $A(0,r) = 1$ we complete the proof.

COROLLARY 4. *If $A(n,r)$ are defined by $(*)$, then for $n \geqq 1$*

$$A(n,r) = \sum_{t=1}^{n} (-1)^{t+1} p^{t(t-1)/2} \begin{bmatrix} p^{n-t}(r-1)+1 \\ t \end{bmatrix} A(n-t,r). \tag{6}$$

PROOF. Since $\left[{r \atop t}\right] = 0$ for $t > r$, and $A(n,r) = 0$ for $n < 0$, (5) can be written as

$$A(n,r) = \sum_{t=1}^{n} (-1)^{t+1} p^{t(t-1)/2} \begin{bmatrix} r \\ t \end{bmatrix} A(n-t,\, p^t(r-1)+1);$$

and the result follows immediately from Lemma 3 by substituting

$$b_t^r = (-1)^{t+1} p^{t(t-1)/2} \begin{bmatrix} r \\ t \end{bmatrix}, \qquad f(r) = p(r-1)+1.$$

REMARK. Lemma 3 can easily be generalized for arbitrary initial conditions.

This result can be generalized to $\widehat{F_r(\mathcal{N})}$, the free pro-nilpotent group on r generators by the following.

LEMMA 5. *If G is a finitely generated group whose finite homomorphic images are nilpotent, and if $n = p_1^{e_1} \cdots p_k^{e_k}$ is the factorization of n into distinct primes, then*

$$a_n = a_{p_1^{e_1}} a_{p_2^{e_2}} \cdots a_{p_k^{e_k}} \qquad (a_n = a_n(G)).$$

(In terms of zeta functions the lemma can be stated as: *The zeta function of G enjoys an Euler product.*)

PROOF. Let $K = \bigcap \{H \leqq G \mid (G:H) \leqq n\}$. K is a characteristic subgroup of finite index, and thus G/K is a finite nilpotent group, so G/K is the direct product of its p-Sylow subgroups. The same applies to every subgroup of G/K, thus the lemma is true for G/K. Applying the homomorphism theorems gives the result for G.

Now recall that $\widehat{F_r(\mathcal{N})} = \Pi_{\text{prime } p} \widehat{F_r(p)}$, and hence we get a recursive formula for $\widehat{F_r(\mathcal{N})}$.

Finally we shall show that $A(n, r)$ has exponential growth as a function of the index p^n; more precisely:

PROPOSITION 6. $\lim_{n \to \infty} (A(n, r))^{p^{-n}} = p^{(r-1)/(p-1)}$.

PROOF. Denote by H the intersection of all maximal subgroups of $\widehat{F_r(p)}$ which contain N, where N is an open subgroup of index p^n. Then $\widehat{F_r(p)}/H$ is an elementary abelian group whose order does not exceed p^n. Hence N is contained in $[{t \atop 1}]$ maximal subgroups of $\widehat{F_r(p)}$ for some $t \leqq n$. We can therefore deduce

$$\frac{A(1, r)A(n-1, p(r-1)+1)}{(p^n - 1)/(p-1)} \leqq A(n, r) \leqq A(1, r)A(n-1, p(r-1)+1),$$

and by induction (substituting $A(1, r) = (p^r - 1)/(p-1)$)

$$p^{(r-1)(p^n-1)/(p-1)-n^2} = \prod_{t=0}^{n-1} \frac{p^{p^t(r-1)}}{p^n} \leqq A(n, r) \leqq \prod_{t=0}^{n-1} \frac{p^{p^t(r-1)+1} - 1}{p-1}$$

$$\leqq \frac{p^n}{(p-1)^n} p^{(r-1)(p^n-1)/(p-1)}$$

and thus $\lim_{n \to \infty} (A(n, r))^{p^{-n}} = p^{(r-1)/(p-1)}$.

REMARK. Proposition 6 implies that every finitely generated pro-p group, G, has at most exponential subgroup growth, thus the series $\Sigma_{n=0}^{\infty} a_n(G)z^n$ defines an analytic function. It is interesting to study the relations between the algebraic structure of G and the analytic properties of this function.

Since $p^{(r-1)/(p-1)} \leqq 2^{r-1}$ for all p, the growth of $a_n(\widehat{F_r(\mathcal{N})})$ is also exponential (more accurately, the growth of $b_n = \Sigma_{k=1}^{n} a_k(\widehat{F_r(\mathcal{N})})$ is exponential). For F_r (the discrete free group on r generators) $a_n(F_r)$ is asymptotic to

$$n(n!)^{r-1} \sim ne^{(n \log n - n)(r-1)} \qquad \text{[Ne]}$$

so the growth in that case is more than exponential.

4. The zeta function of $\mathbf{Z}^r$

Applying the Hall enumeration principle to $\mathbf{Z}^r$ gives:

PROPOSITION 7. *For* $n \geqq 1$

$$a_{p^n}(\mathbf{Z}^r) = a_{p^n} = \sum_{t=1}^{r} (-1)^{t+1} p^{t(t-1)/2} \begin{bmatrix} r \\ t \end{bmatrix} a_{p^{n-t}}.$$

(*For* $n < t$ *we define* $a_{p^{n-t}} = 0$.)

PROOF. Let Φ be given by

$$\Phi = \bigcap \{H \leqq \mathbf{Z}^r \mid (\mathbf{Z}^r : H) = p\}.$$

It is easy to see that the collection of subgroups of index p^n in $\mathbf{Z}^r$ satisfies the conditions of the Hall enumeration principle. Each of the $K_{t,i}$'s is isomorphic to $\mathbf{Z}^r$ and the result follows.

Let $f_{\mathbf{Z}^r}(s)$ be the zeta function of $\mathbf{Z}^r$

$$\left(\text{i.e. } f_{\mathbf{Z}^r}(s) = \sum_{n=1}^{\infty} a_n(\mathbf{Z}^r) n^{-s} = \sum_{n=1}^{\infty} a_n n^{-s}\right).$$

Then $f_{\mathbf{Z}^r}(s)$ enjoys an Euler product, i.e.

$$f_{\mathbf{Z}^r}(s) = \prod_{\text{prime } p} f^p_{\mathbf{Z}^r}(s) = \prod_{\text{prime } p} \left(\sum_{n=0}^{\infty} a_{p^n} p^{-ns}\right).$$

PROPOSITION 8. $f^p_{\mathbf{Z}^r}(s) = \Pi_{t=0}^{r-1} (1 - p^{t-s})^{-1}$.

COROLLARY 9. $f_{\mathbf{Z}^r}(s) = \Pi_{t=0}^{r-1} \zeta(s-t)$, *where* $\zeta(s)$ *is the classical Riemann zeta function*.

PROOF OF PROPOSITION 8. For a constant C_t

$$C_t p^{-ts} f^p_{\mathbf{Z}^r}(s) = \sum_{n=0}^{\infty} C_t a_{p^n} p^{-(n+t)s} = \sum_{n=t}^{\infty} C_t a_{p^{n-t}} p^{-ns} = \sum_{n=0}^{\infty} C_t a_{p^{n-t}} p^{-ns}.$$

(Recall $a_{p^{n-t}} = 0$ for $n < t$.)

The coefficient of p^{-ns} in $\Sigma_{t=0}^{r} C_t p^{-ts} f^p_{\mathbf{Z}}(s)$ is $\Sigma_{t=0}^{r} C_t a_{p^{n-t}}$. Set

$$C_t = (-1)^t p^{t(t-1)/2} \begin{bmatrix} r \\ t \end{bmatrix},$$

and by Proposition 7 we get

$$\left[\sum_{t=0}^{r}(-1)^t p^{t(t-1)/2}\begin{bmatrix} r \\ t \end{bmatrix} p^{-ts}\right] f^p_{\mathbf{Z}^r}(s) = 1.$$

Now from (3) (with the substitution $x = p^s$) we obtain

$$\left[\prod_{t=0}^{r-1}(1 - p^{t-s})\right] f^p_{\mathbf{Z}^r}(s) = 1$$

or $f^p_{\mathbf{Z}^r}(s) = \Pi_{t=0}^{r-1}(1 - p^{t-s})^{-1}$.

The corollary follows since $(1 - p^{t-s})^{-1}$ is the Euler factor of $\zeta(s - t)$.

As was noted in the introduction this result was proved by [BR] and [GSS] using different methods.

5. Non-isomorphic groups with the same zeta function

We shall say that a group G is $f(n)$-indexed if $\mathrm{rk}(K) = f(n)$ for each (open) $K \leqq G$ s.t. $(G : K) = n$ ($\mathrm{rk}(K)$ denotes the minimal number of generators of K). Obviously, if G is $f(n)$-indexed and $(G : K) = k$, then K is $f(nk)$-indexed.

PROPOSITION 10. *If the pro-p groups G_1, G_2 are $f(p^n)$-indexed, then $\zeta_{G_1}(s) = \zeta_{G_2}(s)$. (In other words: $f(p^n)$ determines $\zeta_G(s)$ uniquely.)*

PROOF. Assume $a_{p^i}(G_1) = a_{p^i}(G_2)$ for $i = 0, 1, \ldots, n-1$ for every two pro-p groups G_1, G_2 that are indexed by the same function. Then

$$\begin{aligned} a_{p^n}(G_1) &= \sum_{t=1}^{f(1)}(-1)^{t+1}p^{t(t-1)/2}\sum_{i=1}^{\left[\begin{smallmatrix} f(1) \\ t \end{smallmatrix}\right]} a_{p^{n-t}}(K^1_{t,i}) \\ &= \sum_{t=1}^{f(1)}(-1)^{t+1}p^{t(t-1)/2}\sum_{i=1}^{\left[\begin{smallmatrix} f(1) \\ t \end{smallmatrix}\right]} a_{p^{n-t}}(K^2_{t,i}) = a_{p^n}(G_2). \end{aligned}$$

($K^j_{t,i}$ denotes a subgroup of index p^t in G_j ($j = 1, 2$) containing the Frattini subgroup.)

EXAMPLES.

(1) $f_G(p^n) = p^n(r-1) + 1$

In this case $G \cong \widehat{F_r(p)}$.

PROOF. Let $\varphi : \widehat{F_r(p)} \to G$ be an epimorphism. Since $a_{p^n}(\widehat{F_r(p)}) = a_{p^n}(G)$ for all n, $\ker\varphi \leqq K$ for every open subgroup K of $\widehat{F_r(p)}$, and thus $\ker\varphi = \{1\}$. (This result was first proved in [L] using different methods.)

(2) $f(p^n) = r$

In this case $\zeta_G(s)=\Pi_{i=0}^{r-1}(1-p^{i-s})^{-1}$. We shall consider in detail the case $f(p^n)=2$.

Consider the sequence of groups $M_{1,p}\supset M_{2,p}\supset M_{3,p}\supset\cdots$ defined by

$$M_{k,p}=\left\{\begin{pmatrix} a & A\\ 0 & 1\end{pmatrix}\middle|\, a\in 1+p^k\mathbf{Z}_p, A\in\mathbf{Z}_p\right\}$$

($\mathbf{Z}_p$ denotes the p-adic integers).

It is easy to see that $M_{k,p}$, $M_{l,p}$ are non-isomorphic groups for $k\neq l$ since $M_{k,p}/M'_{k,p}\cong\mathbf{Z}_p\oplus\mathbf{Z}_p/p^k\mathbf{Z}_p$, but they are all 2-indexed (cf. [LM]). (These groups are split extensions of $\mathbf{Z}_p$ by $\mathbf{Z}_p$.) Thus we get an infinite family of pro-p groups with the zeta function $(1/(1-p^s))(1/(1-p^{s-1}))$.

By taking the direct product $\Pi_{\text{prime } p} M_{k,p}$ and permuting the M_k's we can get $2^{\aleph_0}$ non-isomorphic pro-nilpotent groups with the zeta function $\zeta(s)\zeta(s-1)$.

Acknowledgment

This paper was motivated by the author's M.Sc. thesis under the supervision of Prof. A. Lubotzky. I am very grateful for his help and advice. I also want to thank Professor A. Mann for several valuable discussions.

References

[BR] C. J. Bushnell and I. Reiner, *Solomon's conjectures and the local functional equation for zeta functions of orders*, Bull. Am. Math. Soc. **2** (1980), 306–310.

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

[H] M. Hall, *Subgroups of finite index in free groups*, Can. J. Math. **1** (1949), 187–190.

[H2] P. Hall, *A contribution to the theory of groups of prime power order*, Proc. London Math. Soc. (2) **36** (1934), 29–95.

[J] G. A. Jones, *Congruence and non-congruence subgroups of the modular group: A survey*, in Proc. of *Groups St. Andrew 1985* (E. F. Robertson and C. M. Campbell, eds.), London Math. Soc. Lecture Notes Series 121, Cambridge University Press, 1986, pp. 223–234.

[L] A. Lubotzky, *Combinatorial group theory for pro-p groups*, J. Pure Appl. Algebra **25** (1982), 311–325.

[LM] A. Lubotzky and A. Mann, *Powerful p-groups* (2 parts), J. Algebra **105** (1987), 484–515.

[LV] A. Lubotzky and L. van den Dries, *Subgroups of free profinite groups and large subfields of $\tilde{Q}$*, Isr. J. Math. **39** (1981), 25–45.

[Ne] M. Newman, *Asymptotic formulas related to free products of cyclic groups*, Math. Comput. **30** (1976), 838–846.

[S] G. C. Smith, *Zeta functions of torsion free finitely generated nilpotent groups*, Thesis, University of Manchester, 1983.