J. Group Theory **9** (2006), 203–217
DOI 10.1515/JGT.2006.014

**Journal of Group Theory**


# Profinite groups with a rational probabilistic zeta function

Eloisa Detomi and Andrea Lucchini

(Communicated by R. M. Guralnick)

**Abstract.** We discuss whether finiteness properties of a profinite group $G$ can be deduced from the probabilistic zeta function $P_G(s)$. In particular we prove that in the prosoluble case, if $P_G(s)$ is rational then $G/\mathrm{Frat}(G)$ is finite.

## 1 Introduction

Let $G$ be a finitely generated profinite group. As $G$ has only finitely many open subgroups of a given index, for any $n \in \mathbb{N}$ we may define the integer $a_n(G)$ as $a_n(G) = \sum_H \mu_G(H)$, where the sum is over all open subgroups $H$ of $G$ with $|G : H| = n$. Here $\mu_G(H)$ denotes the Möbius function of the poset of open subgroups of $G$, which is defined by recursion as follows: $\mu_G(G) = 1$ and $\mu_G(H) = -\sum_{H<K} \mu_G(K)$ if $H < G$. Then we associate to $G$ a formal Dirichlet series $P_G(s)$, defined as

$$P_G(s) = \sum_{n \in \mathbb{N}} \frac{a_n(G)}{n^s} \quad \text{where} \quad a_n(G) := \sum_{|G:H|=n} \mu_G(H).$$

When $G$ is finite and $t$ is a positive integer, $P_G(t)$ is the probability that $t$ randomly chosen elements generate $G$ (see [7]); the inverse $1/P_G(s)$ is usually called the probabilistic zeta function of $G$ (see Mann [10] and Boston [1]). In the infinite case we do not know whether the series $P_G(s)$ converges (related questions are discussed in [3], [8], [9] and [10]); however in this paper we use the name 'probabilistic zeta function' to indicate the inverse of $P_G(s)$ in the ring of formal Dirichlet series.

Let $\{G_n\}_{n \in \mathbb{N}}$ be a countable descending series of open normal subgroups with the properties that $G_1 = G$, $\bigcap_{n \in \mathbb{N}} G_n = 1$ and $G_n/G_{n+1}$ is a chief factor of $G$ for each $n \in \mathbb{N}$. The factor group $G/G_n$ is finite, and so the Dirichlet series $P_{G/G_n}(s)$ is also finite and belongs to the ring $\mathscr{D}$ of Dirichlet polynomials with integer coefficients. In fact $P_{G/G_n}(s)$ is a divisor of $P_{G/G_{n+1}}(s)$ in the ring $\mathscr{D}$, that is, there exists a Dirichlet

This work is partially supported by MIUR (project Teoria dei gruppi e applicazioni).

polynomial $P_n(s)$ such that $P_{G/G_{n+1}}(s) = P_{G/G_n}(s)P_n(s)$. As explained in [3], the Dirichlet series $P_G(s)$ can be written as an infinite formal product $P_G(s) = \prod_{n\in\mathbb{N}} P_n(s)$, and if we change the series $\{G_n\}_{n\in\mathbb{N}}$, the factorization remains the same up to reordering the factors.

It is possible that a Dirichlet polynomial can be written as a formal product of infinitely many non-trivial elements of $\mathscr{D}$ (for example $1 = (1-2^{-s})\prod_{n\in\mathbb{N}}(1+2^{-2^n s})$). So it is not clear whether the formal series $P_G(s) = \prod_{n\in\mathbb{N}} P_n(s)$ is finite only when $P_n(s) = 1$ for all but finitely many $n \in \mathbb{N}$; more generally we can ask whether one can deduce finiteness properties of $G$ from the fact that $P_G(s)$ is finite. It is not true that if $P_G(s) \in \mathscr{D}$ then $G$ must be finite; indeed $\mu_G(H) \neq 1$ implies that $H$ is an intersection of maximal subgroups and thus $P_G(s) = P_{G/\mathrm{Frat}(G)}(s)$. For example, if $G$ is a free pro-$p$ group of rank $d$ then

$$P_G(s) = P_{(\mathbb{Z}/p\mathbb{Z})^d}(s) = \prod_{0\leqslant i<d} (1-p^i/p^s).$$

However one could conjecture that if $P_G(s) \in \mathscr{D}$ then $G/\mathrm{Frat}(G)$ is finite.

In this paper we mainly deal with prosoluble groups. In this case the polynomials $P_n(s)$ are very simple; indeed $P_n(s) = 1 - c_n/q_n^s$ where $q_n = |G_n/G_{n+1}|$, $c_n$ is a non-negative integer and $c_n = 0$ if and only if $G_n/G_{n+1}$ is a Frattini factor, i.e. $G_n/G_{n+1} \leqslant \mathrm{Frat}(G/G_{n+1})$. In particular, if $G$ is prosoluble (and only in this case, see [4]) $P_G(s)$ has an Euler factorization as $P_G(s) = \prod_p P_{G,p}(s)$ over the set of prime numbers, where

$$P_{G,p}(s) = \sum_{r\in\mathbb{N}} \frac{a_{p^r}(G)}{(p^r)^s} = \prod_{n\in\Omega_p} P_n(s),$$

and, for any prime $p$, $\Omega_p$ is defined as the set of $n \in \mathbb{N}$ such that $G_n/G_{n+1}$ is non-Frattini and has $p$-power order. Therefore, as already noticed by Mann [10], more general questions arise: what can we say about the structure of $G$ if we know that for a certain prime $p$ the Dirichlet series $P_{G,p}(s)$ is a polynomial, and what can we say when $P_{G,p}(s)$ is rational, i.e. $P_{G,p}(s) = A(s)/B(s)$ with $A(s), B(s) \in \mathscr{D}$?

Clearly $P_{G,p}(s)$ is a polynomial when $\Omega_p$ is finite, i.e. when $G$ is virtually pro-($p$-nilpotent). Surprisingly, the converse is not true: in Proposition 6.2 we produce an example of a profinite group $G$ such that, for each prime $p$, the $p$-local factor is a polynomial in $1/p^s$ but $|\Omega_p| = \infty$, i.e. $G$ has infinitely many non-Frattini $p$-chief factors involved in the factorization of $P_{G,p}(s)$; in particular $G$ is not virtually pro-($p$-nilpotent).

The fact that $P_{G,p}(s)$ can be a polynomial even when $\Omega_p$ is infinite might lead one to suspect that there is a counter-example to the conjecture that if $P_G(s) \in \mathscr{D}$ then $G/\mathrm{Frat}(G)$ is finite. However, using results from number theory, we prove that if $P_{G,p}(s)$ is polynomial then either $\Omega_p$ is finite or, for every prime $q$, there exists $n \in \Omega_p$ such that the dimension of $G_n/G_{n+1}$ as $\mathbb{F}_pG$-module is divisible by $q$; using standard arguments of modular representation theory one deduces that this is possible only if

infinitely many primes appear among the divisors of the orders of the finite images of $G$; but then $P_{G,r}(s) \neq 1$ for infinitely many primes $r$ and $P_G(s)$ cannot be polynomial. So $P_G(s)$ can be a polynomial only if $\Omega_p$ is finite for every prime and empty for all but finitely many, and therefore only if $G/\mathrm{Frat}(G)$ is finite. The same argument remains valid under the weaker hypothesis that $P_G(s)$ is rational and $G$ is merely virtually prosoluble instead of prosoluble.

Our main result is the following:

**Main Result** (Theorem 5.4). *If $G$ is a virtually prosoluble finitely generated group, then $P_G(s)$ is rational (or polynomial) only if $G$ has finitely many non-Frattini chief factors, i.e., if and only if $G/\mathrm{Frat}(G)$ is a finite group.*

## 2 Formal Dirichlet series

Let $\mathscr{R}$ be the ring of formal Dirichlet series

$$\mathscr{R} = \left\{ \sum_{n=1}^{\infty} \frac{a_n}{n^s} \mid a_n \in \mathbb{Z} \right\}.$$

Let $\Pi$ be the set of all prime numbers; to each prime $p$ we associate an indeterminate $x_p$ and we consider the isomorphism $\Phi$ between $\mathscr{R}$ and the ring of formal series $\mathbb{Z}[[X_\Pi]]$ on the indeterminates $X_\Pi = \{x_p\}_{p \in \Pi}$ defined by

$$1/p^s \mapsto x_p.$$

Then we say that $\sum_{n=1}^{\infty} a_n/n^s$ is rational if $F(X) = \Phi(\sum_{n=1}^{\infty} a_n/n^s)$ is rational in the ring $\mathbb{Z}[[X_\Pi]]$; this means that there exist polynomials $S(X), Q(X) \in \mathbb{Z}[[X_\Pi]]$ such that $F(X) = S(X)/Q(X)$.

For every prime $p$ we consider the ring homomorphism

$$\Psi_p : \mathbb{Z}[[X_\Pi]] \to \mathbb{Z}[[x_p]] \subseteq \mathbb{Z}[[X_\Pi]]$$

defined by

$$x_p \mapsto x_p, \quad x_q \mapsto 0 \quad \text{for } q \neq p,$$

and we denote by $\Phi_p$ the map $\Psi_p \circ \Phi$.

For a finitely generated profinite group $G$, let

$$P_{G,p}(s) = \sum_{r=0}^{\infty} \frac{a_{p^r}(G)}{(p^r)^s};$$

then $\Phi(P_{G,p}(s)) = \Phi_p(P_G(s))$.

Let $\pi(G)$ be the set of prime divisors of indices of open subgroups of $G$:

$$\pi(G) = \bigcup_{\substack{H \leqslant G \\ |G:H|<\infty}} \pi(|G:H|).$$

**Proposition 2.1.** *Let $G$ be a finitely generated profinite group. Assume that $P_G(s)$ is rational. Then*

(1) *for each $p \in \pi(G)$, $P_{G,p}(s)$ is rational in the ring $\mathbb{Z}[[1/p^s]]$;*

(2) *if $G$ is prosoluble, then $\pi(G)$ is finite.*

*Proof.* (1) If $P_G(s)$ is rational then $\Phi(P_G(s)) = S(X)/Q(X)$ where $S(X)$, $Q(X)$ are polynomials in $\mathbb{Z}[[X_\Pi]]$. Then

$$\Phi(P_{G,p}(s)) = \Phi_p(P_G(s)) = \frac{\Phi_p(S(X))}{\Phi_p(Q(X))},$$

and therefore $P_{G,p}(s)$ is rational in the ring $\mathbb{Z}[[1/p^s]]$.

(2) There exists a finite set of primes $p_1, \dots, p_r$ such that for every prime $q \neq p_1, \dots, p_r$ the polynomials $S(X)$ and $Q(X)$ have zero degree in the indeterminate $x_q$. Then $\Phi(P_{G,q}(s)) = \Phi_q(S(X))/\Phi_q(Q(X))$ is a constant and thus, since $a_1(G) = 1$ by definition, $P_{G,q}(s) = 1$. Let $G$ be a prosoluble group. If $q \in \pi(G)$ then $G$ has a subgroup $M$ of index a power $q^n$ of $q$; when we choose $M$ with $n$ minimal, then $M$, and every subgroup with the same index, is a maximal subgroup of $G$, and thus $\mu_G(M) = -1$ and $a_{q^n}(G) \neq 0$, contradicting $P_{G,q}(s) = 1$. Therefore $\pi(G) \subseteq \{p_1, \dots, p_r\}$.

## 3 Infinite products

The following result is a corollary of the Skolem–Mahler–Lech Theorem (see [11]).

**Proposition 3.1.** *Let $c_1, \dots, c_r$, $\lambda_1, \dots, \lambda_r$ be algebraic numbers with the property that no quotient $\lambda_i/\lambda_j$ is a non-trivial root of unity. Then the exponential polynomial*

$$\psi(m) = c_1\lambda_1^m + \cdots + c_r\lambda_r^m$$

*vanishes for infinitely many integers $m$ only if $\psi(m)$ is identically zero.*

**Proposition 3.2.** *Let $I \subseteq \mathbb{N}$ and let $\{\gamma_i\}_{i\in I}$, $\{n_i\}_{i\in I}$ be positive integers such that*

(i) *for every $n \in \mathbb{N}$, the set $I_n = \{i \in I \mid n_i \text{ divides } n\}$ is finite, and*

(ii) *there exists a prime $q$ such that $q$ does not divide $n_i$ for any $i \in I$.*

*If*

$$F(x) = \prod_{i \in I}(1 - \gamma_i x^{n_i})$$

*is rational in* $\mathbb{Z}[[x]]$, *then* $I = \bigcup_{n \in \mathbb{N}} I_n$ *is finite*.

*Proof.* Hypothesis (i) assures us that $F(x)$ is well defined as a formal power series. Now we study $\log(F(x))$; by formal Taylor expansion of $\log(1 - x)$ we get

$$\begin{aligned}\log(F(x)) &= \log\left(\prod_{i \in I}(1 - \gamma_i x^{n_i})\right) = \sum_{i \in I} \log(1 - \gamma_i x^{n_i}) \\ &= -\sum_{i \in I} \sum_{j=1}^{\infty} \frac{\gamma_i^j (x^{n_i})^j}{j}.\end{aligned}$$

Multiplying the formal derivative of $\log(F(x))$ by $(-x)$ we have

$$-x(\log(F(x)))' = \sum_{i \in I} \sum_{j=1}^{\infty} n_i \gamma_i^j (x^{n_i})^j = \sum_n w(n) x^n,$$

where

$$w(n) = \sum_{i \in I_n} n_i \gamma_i^{n/n_i}. \tag{3.1}$$

Since $F(x)$ is rational, there are polynomials $S(x)$, $Q(x)$ in $\mathbb{Z}[x]$ such that $F(x) = S(x)/Q(x)$. Let

$$S(x) = (1 - \alpha_1 x) \dots (1 - \alpha_s x) \quad \text{and} \quad Q(x) = (1 - \beta_1 x) \dots (1 - \beta_r x)$$

for complex numbers $\alpha_i, \beta_j$, $i = 1, \dots, s$, $j = 1, \dots, r$. Hence

$$\begin{aligned}\log(F(x)) &= \log\left(\frac{(1 - \alpha_1 x) \dots (1 - \alpha_s x)}{(1 - \beta_1 x) \dots (1 - \beta_r x)}\right) \\ &= \sum_{i=1}^{s} \log(1 - \alpha_i x) - \sum_{l=1}^{r} \log(1 - \beta_l x) \\ &= -\sum_{i,j} \frac{\alpha_i^j x^j}{j} + \sum_{l,j} \frac{\beta_l^j x^j}{j}\end{aligned}$$

and

$$-x(\log(F(x)))' = \sum_{i,j} \alpha_i^j x^j - \sum_{l,j} \beta_l^j x^j = \sum_n w(n) x^n,$$

where

$$w(n) = \alpha_1^n + \cdots + \alpha_s^n - \beta_1^n - \cdots - \beta_r^n. \tag{3.2}$$

Comparing (3.1) and (3.2), we obtain, for every $n \in \mathbb{N}$, the following identity:

$$\alpha_1^n + \cdots + \alpha_s^n - \beta_1^n - \cdots - \beta_r^n = \sum_{i \in I_n} n_i \gamma_i^{n/n_i}. \tag{3.3}$$

Replacing in (3.3) $n$ by $mn$, we have

$$\sum_{i=1}^{s} (\alpha_i^n)^m - \sum_{i=1}^{r} (\beta_i^n)^m - \sum_{i \in I_n} n_i (\gamma_i^{n/n_i})^m = \sum_{i \in I_{nm} \setminus I_n} n_i \gamma_i^{nm/n_i}. \tag{3.4}$$

Thus the exponential polynomial

$$\psi_n(m) = \sum_{i=1}^{s} (\alpha_i^n)^m - \sum_{i=1}^{r} (\beta_i^n)^m - \sum_{i \in I_n} n_i (\gamma_i^{n/n_i})^m \tag{3.5}$$

can be written, by (3.4), as

$$\psi_n(m) = \sum_{i \in I_{nm} \setminus I_n} n_i \gamma_i^{nm/n_i}. \tag{3.6}$$

Let

$$\Lambda_n = \{\alpha_1^n, \ldots, \alpha_s^n, \beta_1^n, \ldots, \beta_r^n, \gamma_i^{n/n_i} \mid i \in I_n\}.$$

To apply Proposition 3.1 to the exponential polynomial $\psi_n(m)$ we have to choose an integer $n$ such that no ratio of two elements in $\Lambda_n$ is a non-trivial root of unity. So define $\Omega$ to be the set of roots of unity of the form $\omega = x/y$ with $x, y \in \{\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_r\}$ and let $e$ be the order of the group generated by $\Omega$. Then a ratio of elements of $\Lambda_e = \{\alpha_1^e, \ldots, \alpha_s^e, \beta_1^e, \ldots, \beta_r^e, \gamma_i^{e/n_i} \mid i \in I_e\}$ is a non-trivial root of unity only if it is $\alpha_j^e/\gamma_i^{e/n_i}$ or $\beta_k^e/\gamma_i^{e/n_i}$ for some $i \in I_e$. As each $\gamma_i$ is a positive integer, we can choose an integer $d > 0$ such that for every $x \in \Lambda_e$ the following holds:

$$\text{if } (x^d)^m \in \mathbb{N} \text{ for some } m \in \mathbb{N} \text{ then } x^d \in \mathbb{N}.$$

Hence, for $n = ed$, the set $\Lambda_n$ contains no pair of elements whose ratio is a non-trivial root of unity.

By (ii) there exists a prime $q$ such that $q$ does not divide $n_i$ for every $i \in I$; this implies that

$$I_{nq^c} = I_n \quad \text{for every } c \in \mathbb{N}.$$

Therefore, by equation (3.6),

$$\psi_n(q^r) = 0 \quad \text{for every } r \in \mathbb{N},$$

and so the exponential polynomial $\psi_n(m)$ vanishes for infinitely many integers. Hence $\psi_n(m)$ satisfies the hypothesis of Proposition 3.1 and thus

$$\psi_n(m) = 0 \quad \text{for every } m \in \mathbb{N}.$$

Then, by the identity (3.4), we obtain that

$$\sum_{i \in I_{nm} \setminus I_n} n_i \gamma_i^{nm/n_i} = 0 \quad \text{for every } m \in \mathbb{N},$$

and, since each $\gamma_i$ is a positive integer, we have

$$I_{nm} = I_n \quad \text{for every } m \in \mathbb{N}.$$

Since every $i \in I$ belongs to $I_{nn_i}$, it follows that $I = I_n$. Then, by (i), $I$ is finite and this completes the proof.

An infinite product of non-trivial polynomials may be rational. We give the following known example (see e.g. [12, Chapter 4, Example 4]) which will be used in the last section.

**Lemma 3.3.** *There exists a sequence $(t_i)_{i \in \mathbb{N}}$ of positive integers such that*

(i) $1 - 2x = \prod_{i=1}^{\infty} (1 - x^i)^{t_i}$, *and*

(ii) $0 \leqslant t_i \leqslant 2^i$.

*Proof.* Applying the function log to the equation $(1 - 2x) = \prod_{i=1}^{\infty} (1 - x^i)^{t_i}$ we obtain that

$$\log(1 - 2x) = \sum_{i=1}^{\infty} t_i \log(1 - x^i)$$

and, by a formal power series expansion of $\log(1 - x)$, we have

$$-\sum_n 2^n \frac{x^n}{n} = -\sum_i t_i \sum_j \frac{x^{ij}}{j}. \tag{3.7}$$

Taking formal derivatives of the two sides of (3.7) we see that

$$-\sum_n 2^n x^{n-1} = -\sum_i t_i \sum_j i \cdot x^{ij-1}$$

and multiplying this equation by $(-x)$, we obtain that

$$\sum_n 2^n x^n = \sum_i \sum_j t_i i \cdot x^{ij} = \sum_n \sum_{i \text{ divides } n} t_i i \cdot x^n.$$

Comparing the coefficients of $x^n$ we have

$$2^n = \sum_{i \text{ divides } n} t_i i. \tag{3.8}$$

Applying the Möbius inversion formula, we deduce that

$$t_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) 2^d;$$

it is well known that $t_n$ is the number of irreducible polynomials in $\mathbb{F}_2[x]$ of degree $n$, and so it is an integer and is at most $2^n$.

## 4 The main theorem for prosoluble groups

In order to make our exposition clearer we shall now prove our main theorem for prosoluble groups. We defer to the next section the small changes needed for the proof in the virtually prosoluble case.

**Lemma 4.1.** *Let $n$ be the degree of an irreducible linear representation over a finite field $F$ of a finite $p$-soluble group $G$, where $p = \mathrm{char}(F)$. Then $n$ divides $|G|\varphi(\exp(G))$. In particular, if $q$ is a prime divisor of $n$, then $q \leqslant \max\{\pi(G)\}$.*

*Proof.* By a result of Brauer (see e.g. [5, (A 5.21)]) there exists a field extension $L$ of $F$ such that $L$ is a splitting field for $G$ and all of its subgroups, and the degree $|L : F|$ divides $\varphi(\exp(G))$. Let $V = F^n$ be an irreducible $FG$-module of dimension $n$ and let $W$ be an irreducible constituent of $V_L = V \otimes_F L$. Then $\dim_F(V) = n = r \cdot \dim_L(W)$ where $r$ divides $|L : F|$ and hence $\varphi(\exp(G))$ (see e.g. [5, (A 5.15)]).

Moreover, since $G$ is $p$-soluble and $L$ is a splitting field for $G$, by a result of Fong, Swang and Rukolaine (see e.g. [5, (A 7.14)]) the dimension of the irreducible $LG$-module $W$ divides $|G|$. This implies that $n$ divides $|G|\varphi(\exp(G))$.

Finally, if $\pi(G) = \{p_1, \ldots, p_r\}$ and $\exp(G) = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, then

$$\varphi(\exp(G)) = \prod_{\alpha_i \neq 0} (p_i - 1) p_i^{\alpha_i - 1}.$$

Therefore each prime divisor of $n$ divides $|G|\varphi(\exp(G))$ and so is bounded by $\max\{\pi(G)\}$.

A finitely generated profinite group has a countable chief series, that is, a countable descending series $\{G_n\}_{n\in\mathbb{N}}$ of open normal subgroups such that $G_1 = G$, $\bigcap_{n\in\mathbb{N}} G_n = 1$ and $G_n/G_{n+1}$ is a chief factor of $G$ for each $n \in \mathbb{N}$.

**Proposition 4.2.** *Let $G$ be a finitely generated prosoluble group and let $p \in \pi(G)$. If*

(1) *$P_{G,p}(s)$ is rational in $\mathbb{Z}[[1/p^s]]$, and*

(2) *$\pi(G)$ is finite,*

*then in each chief series of $G$ there are only finitely many non-Frattini chief factors of $p$-power order.*

*Proof.* Let $\{V_i\}_{i\in I}$ be the set of all non-Frattini $p$-chief factors in a chief series of $G$ and let $n_i = \dim_{\mathbb{F}_p}(V_i)$, where $\mathbb{F}_p$ is the field with $p$ elements. By a result of Gaschütz (see [6]),

$$P_{G,p}(s) = \prod_{i\in I}(1 - c_i/p^{n_i s})$$

for some positive integers $c_i \in \mathbb{N}$, and moreover the set $I_n = \{i \in I \mid n_i \text{ divides } n\}$ is finite for every integer $n$.

Since each $n_i$ is in fact the degree of an irreducible linear representation of a finite soluble homomorphic image of $G$, we deduce by Proposition 4.1 that the prime divisors of the numbers $n_i$ are bounded by the largest prime in $\pi(G)$.

Then the formal product

$$\Phi(P_{G,p}(s)) = \prod_{i\in I}(1 - c_i x_p^{n_i})$$

is rational in $\mathbb{Z}[[x_p]]$ and there exists a prime $q > \max\{\pi(G)\}$ such that $q$ does not divide $n_i$ for any $i \in I$. Thus by Proposition 3.2 it follows that $I$ is finite and this completes the proof.

**Theorem 4.3.** *Let $G$ be a finitely generated prosoluble group and let* $\mathrm{Frat}(G)$ *be its Frattini subgroup. Then the following are equivalent*:

(1) *there exists an integer $\bar{n}$ such that $a_n(G) = 0$ for every $n > \bar{n}$;*

(2) *$P_G(s)$ is polynomial*;

(3) *$P_G(s)$ is rational*;

(4) *$G/\mathrm{Frat}(G)$ is finite.*

*Proof.* The only non-trivial implication is (3) $\Rightarrow$ (4). So let $P_G(s)$ be rational; by Proposition 2.1 it follows that $\pi(G)$ is finite and that $P_{G,p}(s)$ is a rational function for every prime $p \in \pi(G)$. Then by Proposition 4.2 we deduce that each chief series of $G$ has only finitely many non-Frattini chief factors. Thus there exists a normal subgroup $N$ of finite index in $G$ such that every chief factor of $G$ contained in $N$ is Frattini. Hence $N \leqslant \mathrm{Frat}(G)$: indeed in every finite homomorphic image $\overline{G}$ of $G$, each $\overline{G}$-chief factor of $\overline{N}$ is Frattini and this implies that $\overline{N} \leqslant \mathrm{Frat}(\overline{G})$. Therefore $\mathrm{Frat}(G)$ has finite index in $G$ and this completes the proof.

## 5 Virtually prosoluble groups

To deal with virtually prosoluble groups we need to recall some more properties of the series $P_G(s)$ (see also [2], [3]). Let $G$ be a profinite group and let $N$ be a normal open subgroup of $G$. Then $P_G(s)$ has a factorization in the ring of formal Dirichlet series as

$$P_G(s) = P_{G/N}(s)P_{G,N}(s)$$

where

$$P_{G,N}(s) = \sum_{n \in \mathbb{N}} \frac{b_n(G,N)}{n^s} \quad \text{for } b_n(G,N) := \sum_{\substack{|G:H|=n,\\ HN=G}} \mu_G(H).$$

By taking a chief series $\{G_i\}_{i \in \mathbb{N}}$ of $G$, we obtain a factorization of $P_G(s)$ as a formal product of Dirichlet polynomials $P_i(s) = P_{G/G_{i+1}, G_i/G_{i+1}}(s)$ corresponding to non-Frattini chief factors $G_i/G_{i+1}$:

$$P_G(s) = \prod_{i \in \mathbb{N}} P_i(s) = \prod_{i \in \mathbb{N}} P_{G/G_{i+1}, G_i/G_{i+1}}(s). \tag{5.1}$$

As this factorization does not depend on the chief series, we can assume that $N = G_m$ for some integer $m$ and thus we obtain a factorization of $P_{G,N}(s)$. If the chief factor $G_n/G_{n+1}$ is soluble, then the polynomial $P_n(s)$ has a simple expression: $P_n(s) = 1 - c_n/q_n^s$ where $q_n = |G_n/G_{n+1}|$, $c_n$ is a non-negative integer and $c_n = 0$ if and only if $G_n/G_{n+1}$ is a Frattini factor. In particular, if $N$ is prosoluble $P_{G,N}(s)$ has an Euler factorization as $P_{G,N}(s) = \prod_p P_{G,N,p}(s)$ for primes $p$ where

$$P_{G,N,p}(s) = \sum_{r \in \mathbb{N}} \frac{b_{p^r}(G,N)}{(p^r)^s} = \prod_{n \in \Omega_{N,p}} P_n(s) \tag{5.2}$$

and $\Omega_{N,p}$ is defined as the set of $n \in \mathbb{N}$ such that $G_n/G_{n+1}$ is a non-Frattini $p$-chief factor contained in $N$.

**Proposition 5.1.** *Let $G$ be a virtually prosoluble finitely generated group and $N$ a prosoluble open normal subgroup. Assume that $P_G(s)$ is rational. Then*

(1) *$P_{G,N,p}(s)$ is rational in the ring $\mathbb{Z}[[1/p^s]]$, for $p$ prime;*

(2) *$\pi(G)$ is finite.*

*Proof.* Since $G/N$ is finite, $P_{G/N}(s)$ is a polynomial and the formal series $P_{G,N}(s) = P_G(s)/P_{G/N}(s)$ is rational; say $\Phi(P_{G,N}(s)) = S(X)/Q(X)$ where $S(X)$ and $Q(X)$ are polynomials. As in the proof of Proposition 2.1, it follows that $P_{G,N,p}(s)$ is rational in the ring $\mathbb{Z}[[1/p^s]]$ and, if $p_1, \ldots, p_r$ are the primes such that the only indeterminates appearing in $S(X)$ and $Q(X)$ with positive exponent are $x_{p_1}, \ldots, x_{p_r}$, then for $q \neq p_1, \ldots, p_r$ we have $P_{G,N,q}(s) = 1$.

Let $\{G_n\}_{n \in \mathbb{N}}$ be a chief series of $G$. We can assume that $N = G_m$ for an integer $m$. Let $q \in \pi(G)$ be a prime such that $q$ does not divides $G/N$; then $q$ divides the order of a chief factor $G_n/G_{n+1}$ for some $n \geqslant m$, and thus $G_n \leqslant N$. Let $n$ be the minimal integer such that $q$ divides $|G_n/G_{n+1}|$. Since $N$ is soluble, $G_n/G_{n+1}$ is an elementary abelian $q$-group and, by minimality of $n$, its order is prime to its index in $G$; therefore by the Schur–Zassenhaus theorem there exists a complement to $G_n/G_{n+1}$ in $G/G_{n+1}$. This implies that the set $\Omega$ of subgroups with $q$-power index in $G$ and supplementing $N$ is non-empty. Let $q^\alpha$ be the minimal index of a subgroup in $\Omega$; then every subgroup $M$ in $\Omega$ with index $q^\alpha$ is a maximal subgroup and therefore

$$b_{q^z}(G,N) = \sum_{M \in \Omega} \mu_G(M) \neq 0.$$

Hence $P_{G,N,q}(s) \neq 1$ and thus $q \in \{p_1, \ldots, p_r\}$. Then we conclude that

$$\pi(G) \subseteq \{p_1, \ldots, p_r\} \cup \pi(|G/N|).$$

**Lemma 5.2.** *Let $N$ be a soluble normal subgroup of index $a$ in a finite group $G$ and let $n$ be the degree of an irreducible linear representation of $G$ over a finite field $F$. If $q$ is a prime divisor of $n$, then $q \leqslant \max\{p, a \mid p \in \pi(G)\}$.*

*Proof.* Let $V = F^n$ be an irreducible $FG$-module of dimension $n$ and let $W$ be an irreducible constituent of $V_N$. By Clifford's Theorem, $V_N$ is the direct sum of $r$ irreducible $N$-modules $F$-isomorphic to $W$, where $r \leqslant |G:N| = a$. Thus $\dim_F(V) = n = r \dim_F(W)$, and a prime divisor $q$ of $n$ divides either $\dim_F(W)$ or $r$. If $q$ divides $r$, then $q \leqslant a$. Otherwise $q$ divides $\dim_F(W)$: as $N$ is soluble and $W$ is irreducible, Lemma 4.1 gives that $q$ is bounded by $\max\{\pi(N)\} \leqslant \max\{\pi(G)\}$, and the lemma is proved.

Using the last lemma and arguing as in Proposition 4.2, we obtain the following:

**Proposition 5.3.** *Let $N$ be a prosoluble open normal subgroup of a profinite group $G$*

*and let* $p \in \pi(G)$. *If* $P_{G,N,p}(s)$ *is rational in* $\mathbb{Z}[[1/p^s]]$ *and* $\pi(G)$ *is finite then in every chief series of* $G$ *there are only finitely many non-Frattini chief factors of* $p$*-power order*.

Combining Propositions 5.1 and 5.3, we obtain the extension of Theorem 4.3 to virtually prosoluble groups:

**Theorem 5.4.** *Let* $G$ *be a finitely generated virtually prosoluble group. Then the following are equivalent*:

(1) *there exists an integer* $\bar{n}$ *such that* $a_n(G) = 0$ *for every* $n > \bar{n}$;

(2) $P_G(s)$ *is polynomial*;

(3) $P_G(s)$ *is rational*;

(4) $G/\mathrm{Frat}(G)$ *is finite*.

## 6 A rational $P_{G,p}(s)$

Generalizing a property of nilpotent groups, Mann [10] proved the following result.

**Proposition 6.1** ([10]). *If* $G$ *is a finitely generated prosoluble virtually* $p$*-nilpotent group, then* $P_{G,p}(s)$ *is a polynomial in the indeterminate* $1/p^s$.

Whether the converse holds was left open (see [9]). Using Lemma 3.3, we can give a counter-example which also shows that if $\pi(G)$ is not finite, then the conclusion of Proposition 4.2 no longer holds; indeed $P_{G,p}(s)$ can be rational with 'infinitely many non-trivial factors'.

To construct such a group we need to state explicitly the already cited result of Gaschütz [6]. Let $A = G_i/G_{i+1}$ be an abelian non-Frattini chief factor of a profinite group $G$. Then the Dirichlet polynomial that appears in the product 5.1 is precisely

$$P_i(s) = P_{G/G_{i+1},\, G_i/G_{i+1}}(s) = 1 - \frac{|\mathrm{End}_G(A)|^{\delta_{G/G_{i+1}}(A)-1}|A|^{\theta_G(A)}}{|A|^s} \tag{6.1}$$

where $\delta_{G/G_{i+1}}(A)$ is the number of non-Frattini chief factors of $G/G_{i+1}$ that are $G$-isomorphic to $A$, and $\theta_G(A) = 1$ if $A$ is a non-trivial $G$-module, and 0 otherwise.

**Proposition 6.2.** *There exists a finitely generated prosoluble group* $G$ *such that for every prime* $p$

(1) $P_{G,p}(s)$ *is a polynomial, and*

(2) $G$ *has infinitely many non-Frattini chief factors that are* $p$*-groups*.

*Proof.* Let $H = \hat{\mathbb{Z}}^{(2)}$ be the profinite completion of $\mathbb{Z} \times \mathbb{Z}$. Then

$$P_H(s) = \zeta(s)\zeta(s-1) = \prod_{p \in \Pi}(1 - 1/p^s)(1 - p/p^s),$$

where $\zeta(s)$ is the Riemann zeta function (see e.g. [8, Chapter 11]).

Let us fix a prime $p$. For every integer $n$, the multiplicative group of the finite field $\mathbb{F}_q$ with $q = p^n$ elements acts by right multiplication on the additive group $(\mathbb{F}_q, +)$, which can be viewed as a vector space of dimension $n$ over $\mathbb{F}_p$; hence the cyclic group $C_{p^n-1}$ has an irreducible representation of degree $n$ over $\mathbb{F}_p$. Since $H$ has at least $p^n - 1$ normal subgroups $K_i$ with $H/K_i \cong C_{p^n-1}$, there are at least $p^n - 1$ irreducible $H$-modules, say $M_{p,n,i}$, with $1 \leqslant i \leqslant p^{n-1}$, obtained by extending to $H$ the action of $\mathbb{F}_q^*$ on $\mathbb{F}_p^n$ via the isomorphism $\psi_i : H/K_i \to \mathbb{F}_q^*$; note that the $H$-modules $M_{p,n,i}$ are pairwise inequivalent, since they have distinct centralizers $K_i$ in $H$.

Let $\{t_i\}_{i \in \mathbb{N}}$ be the set of integers defined in Lemma 3.3. Since $t_n \leqslant 2^n \leqslant p^n - 1$ if $p$ is odd and $t_n \leqslant 2^{2n} - 1$, for every integer $n$ and each prime $p$ we can consider the following $t_n$ pairwise non-isomorphic irreducible $H$-modules:

$$M_{p,n,1}, \ldots, M_{p,n,t_n}, \quad \text{for } p \neq 2,$$
$$M_{2,2n,1}, \ldots, M_{2,2n,t_n}, \quad \text{for } p = 2.$$

Note that $|M_{p,n,i}| = p^n$ for $p \neq 2$ and $|M_{2,2n,i}| = 4^n$.

We form the $H$-module obtained as the Cartesian product

$$M = \prod_{\substack{n \in \mathbb{N}, \\ i=1,\ldots,t_n}} M_{2,2n,i} \times \prod_{\substack{p \text{ prime} \neq 2, \\ n \in \mathbb{N}, \\ i=1,\ldots,t_n}} M_{p,n,i}$$

of the $H$-modules $M_{p,n,i}$ and $M_{2,2n,i}$ for every prime $p$, every positive integer $n$ and $1 \leqslant i \leqslant t_n$; we define $G$ to be the semidirect product of $H$ acting on the $H$-module $M$:

$$G = H \ltimes M.$$

For a given prime $p$ and a fixed chief series of $G$, we look for the non-Frattini factors whose order is a $p$-power. There are two central factors of order $p$ in $G/M = H$; moreover for any $n \in \mathbb{N}$ there are exactly $t_n$ non-central factors whose order is $p^n$ if $p \neq 2$ and $4^n$ otherwise, corresponding to $M_{p,n,i}$ and $M_{2,2n,i}$, respectively. The non-central factors are pairwise non-isomorphic as $G$-modules, and so from (6.1) we deduce that if $G_i/G_{i+1}$ is one of the $t_n$ non-Frattini chief factors $G$-isomorphic to $M_{p,n,i}$, or $M_{2,2n,i}$, then

$$P_{G/G_{i+1}, G_i/G_{i+1}}(s) = \begin{cases} 1 - \frac{p^n}{p^{ns}} & \text{for } p \neq 2, \\ 1 - \frac{4^n}{4^{ns}} & \text{for } p = 2. \end{cases}$$

It follows that the factorization of $P_{G,p}(s)$ corresponding to a chief series is the following:

$$P_{G,p}(s) = \begin{cases} (1-1/p^s)(1-p/p^s)\prod_{n>0}\left(1-\frac{p^n}{(p^n)^s}\right)^{t_n} & \text{for } p \neq 2, \\ (1-1/2^s)(1-2/2^s)\prod_{n>0}\left(1-\frac{4^n}{(4^n)^s}\right)^{t_n} & \text{for } p = 2. \end{cases} \tag{6.2}$$

Then, by Lemma 3.3, we obtain that $P_{G,p}(s)$ is a polynomial for every prime $p$:

$$P_{G,p}(s) = \begin{cases} (1-1/p^s)(1-p/p^s)(1-2p/p^s) & \text{for } p \neq 2, \\ (1-1/2^s)(1-2/2^s)(1-8/4^s) & \text{for } p = 2. \end{cases}$$

Note that $G$ is 2-generated. Indeed if $N$ is an open normal subgroup of $G$ then $P_{G/N,p}(s)$ is the product of finitely many of the factors involved in (6.2), and hence

$$P_{G/N}(2) = \prod_{p \in \pi(G/N)} P_{G/N,p}(2) > 0$$

and $G/N$ is 2-generated.

Thus $G$ has the desired properties and the proof of the theorem is complete.

For the sake of completeness we notice that in the case when $\pi(G)$ is finite and $G$ is soluble there is a converse to Proposition 6.1:

**Proposition 6.3.** *Let $G$ be a profinite pro-($p$-soluble) finitely generated group such that there exists a prime $q$ which is not a prime divisor of $(1-r)r$ for any prime $r \in \pi(G)$. If $P_{G,p}(s)$ is rational, then $G$ is virtually $p$-nilpotent.*

*Proof.* By the same argument as in Proposition 4.2 we have that a chief series of $G$ contains only a finite number of non-Frattini $p$-factors. The centralizer of all of these $p$-chief factors is of finite index in $G$ and is $p$-nilpotent.

## References

[1] N. Boston. A probabilistic generalization of the Riemann zeta function. *Analytic Number Theory* **1** (1996), 155–162.
[2] E. Detomi and A. Lucchini. Crowns and factorization of the probabilistic zeta function of a finite group. *J. Algebra* **265** (2003), 651–668.
[3] E. Detomi and A. Lucchini. Crowns in profinite groups and applications. Preprint.
[4] E. Detomi and A. Lucchini. Profinite groups with multiplicative probabilistic zeta function. *J. London Math. Soc.* (2) **70** (2004), 165–181.
[5] K. Doerk and T. O. Hawkes. *Finite soluble groups* (de Gruyter, 1992).
[6] W. Gaschütz. Die Eulersche Funktion endlicher auflösbarer Gruppen. *Illinois J. Math.* **3** (1959), 469–476.
[7] P. Hall. The Eulerian functions of a group. *Quart. J. Math.* (*Oxford Ser.*) **7** (1936), 134–151.

[8] A. Lubotzky and D. Segal. *Subgroup growth* (Birkhäuser Verlag, 2003).
[9] A. Mann. A probabilistic zeta function for arithmetic groups. *Internat. J. Algebra Comput*, to appear.
[10] A. Mann. Positively finitely generated groups. *Forum Math.* **8** (1996), 429–459.
[11] A. J. van der Poorten. Some facts that should be better known, especially about rational functions. In *Number theory and applications (Banff, AB, 1988)* (Kluwer, 1989), pp. 497–528.
[12] P. Stanley. *Enumerative combinatorics*, vol. 1 (Cambridge University Press, 1997).

Received 4 February, 2005

Andrea Lucchini, Dipartimento di Matematica, Università di Brescia, Via Valotti, 9, 25133 Brescia, Italy
E-mail: lucchini@ing.unibs.it

Eloisa Detomi, Dipartimento di Matematica Pura ed Applicata, Università di Padova, via Belzoni, 7, 35131 Padova, Italy
E-mail: detomi@math.unipd.it