J. Group Theory **10** (2007), 453–466
DOI 10.1515/JGT.2007.038

Journal of Group Theory

Non-prosoluble profinite groups with a rational probabilistic zeta function

Eloisa Detomi and Andrea Lucchini

(Communicated by R. M. Guralnick)

Abstract. We discuss finiteness properties of a profinite group G whose probabilistic zeta function $P_G(s)$ is rational. In particular we prove that if $P_G(s)$ is rational and G has a finite number of non-alternating and non-abelian composition factors in a given composition series, then $G/\mathrm{Frat}(G)$ is finite.

1 Introduction

To a finitely generated profinite group G we associate a formal Dirichlet series $P_G(s)$, defined as

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

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 $H < G$. We do not know whether the series $P_G(s)$ converges (related questions are discussed in [1], [6], [7] and [8]), however in this paper we just use the name 'probabilistic zeta function' to indicate the inverse of $P_G(s)$ in the ring of formal Dirichlet series.

In [3] we conjectured that if $P_G(s)$ is rational (i.e. if it is a quotient $A(s)/B(s)$ with $A(s)$, $B(s)$ Dirichlet polynomials with integer coefficients) then $G/\mathrm{Frat}(G)$ is a finite group, and we proved this conjecture in the particular case of prosoluble groups. Our aim is now to generalize this result to a wider class of profinite groups.

Let $\{G_i\}_{i \in \mathbb{N}}$ be a countable descending series of open normal subgroups with the properties that $G_1 = G$, $\bigcap_{i \in \mathbb{N}} G_i = 1$ and G_i/G_{i+1} is a chief factor of G for each $i \in \mathbb{N}$. As explained in [1], to each chief factor G_i/G_{i+1} of G we can associate a Dirichlet polynomial $P_i(s)$ such that $P_G(s)$ can be written as an infinite formal product

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

$$P_G(s) = \prod_{i \in \mathbb{N}} P_i(s).$$

In the prosolvable case the polynomials $P_i(s)$ are very simple; indeed $P_i(s) = 1 - c_i/q_i^s$ where $q_i = |G_i/G_{i+1}|$, c_i is a non-negative integer and $c_i = 0$ if and only if G_i/G_{i+1} is a Frattini factor, i.e. $G_i/G_{i+1} \leqslant \mathrm{Frat}(G/G_{i+1})$. In particular, if G is prosoluble, then $P_G(s)$ has an Euler factorization over the set of prime numbers and, given that $P_G(s)$ is rational, each Euler factor is rational and $\pi(G)$ is finite (where $\pi(G)$ is the set of primes involved in the factorization of the indices of the open subgroups of G). Working on each Euler factor we were able to prove that if $P_G(s)$ is rational, then $P_i(s) = 1$ for all but a finite number of $i \in \mathbb{N}$; equivalently almost every chief factor G_i/G_{i+1} is a Frattini factor, and this implies that $G/\mathrm{Frat}(G)$ is finite.

Unfortunately, when G is not prosoluble there is no such nice Euler factorization of $P_G(s)$ and in addition the factors $P_i(s)$ are not such simple polynomials. So, even the first natural question, to deduce the finiteness of $\pi(G)$ from the rationality of $P_G(s)$, seems to be a hard problem for non-prosoluble groups. However we do obtain a kind of Euler factorization over the finite simple groups by collecting together, for each simple group S, all factors $P_i(s)$ such that G_i/G_{i+1} is isomorphic to a direct product of copies of S:

$$P_G(s) = \prod_{S \text{ simple}} E_S(s), \quad \text{where } E_S(s) = \prod_{G_i/G_{i+1} \cong S^{r_i}} P_i(s).$$

At this point we have several unsolved problems: we do not know whether there are finitely many Euler factors $E_S(s)$; we cannot infer from the rationality of $P_G(s)$ that each Euler factor $E_S(s)$ is rational, indeed products of non-rational series might be rational; even if an Euler factor $E_S(s)$ is rational, we cannot deduce from this that there are only finitely many chief factors $G_i/G_{i+1} \cong S^{r_i}$ corresponding to it.

In this paper we analyze the case when, for all but a finite number of indices i, the factors G_i/G_{i+1} are either abelian or direct products of alternating groups. By a close investigation of subgroup indices in alternating groups, and some new reduction techniques we obtain the following result:

Main Result (Theorem 6.1). *Let G be a finitely generated profinite group such that almost every composition factor is cyclic or isomorphic to an alternating group. Then $P_G(s)$ is rational only if $G/\mathrm{Frat}(G)$ is a finite group (and in this case $P_G(s)$ is a Dirichlet polynomial).*

2 Notation and preliminary results

Let G be a finitely generated profinite group and let $\{G_i\}_{i \in \mathbb{N}}$ be a fixed countable descending series of open normal subgroups with the properties that $G_1 = G$, $\bigcap_{i \in \mathbb{N}} G_i = 1$ and G_i/G_{i+1} is a chief factor of G. For each $i \in \mathbb{N}$ there exist a simple group S_i and a positive integer r_i such that $G_i/G_{i+1} \cong S_i^{r_i}$. Moreover, as described in [1], for each $i \in \mathbb{N}$, a finite Dirichlet series

$$P_i(s) = \sum_{n \in \mathbb{N}} \frac{b_{i,n}}{n^s} \tag{2.1}$$

is associated with the chief factor G_i/G_{i+1} and $P_G(s)$ can be written as an infinite formal product of the finite Dirichlet series $P_i(s)$:

$$P_G(s) = \prod_{i \in \mathbb{N}} P_i(s).$$

We recall some properties of the series $P_i(s)$. If S_i is cyclic of prime order p_i, then $P_i(s) = 1 - c_i/(p_i^{r_i})^s$, where c_i is the number of complements of G_i/G_{i+1} in G/G_{i+1}. It is more difficult to compute the series $P_i(s)$ when S_i is a non-abelian simple group. In this case an important role is played by the group $L_i = G/C_G(G_i/G_{i+1})$. This is a monolithic primitive group whose unique minimal normal subgroup is isomorphic to $G_i/G_{i+1} \cong S_i^{r_i}$. If $n \neq |S_i|^{r_i}$, then the coefficient $b_{i,n}$ in (2.1) depends only on L_i; more precisely we have

$$b_{i,n} = \sum_{\substack{|L_i:H|=n \\ L_i = H \operatorname{soc}(L_i)}} \mu_{L_i}(H).$$

It is not easy to compute the coefficient $b_{i,n}$ even for $n \neq |S_i|^{r_i}$. Some help comes from knowledge of the subgroup X_i of $\operatorname{Aut} S_i$ induced by the conjugation action of the normalizer in L_i of a composition factor of the socle S_i^r (note that X_i is an almost simple group with socle isomorphic to S_i). Let us describe some results that one can apply in this context.

Let L be a monolithic primitive group with $N = \operatorname{soc} L = T_1 \times \cdots \times T_r$ and $T_i \cong S$ a finite non-abelian simple group and let X be the subgroup of $\operatorname{Aut} S$ induced by the conjugation action of $N_L(T_1)$ on T_1. As described in [2, Section 1], L can be viewed as a subgroup of $X \wr \operatorname{Sym}(r)$, with $N = \operatorname{soc} L = S^r$ contained in the base X^r of this wreath product. To compute the number

$$b_n = \sum_{\substack{|L:H|=n \\ L=HN}} \mu_L(H), \quad \text{for } n \neq |S|^r,$$

we have to consider only the subgroups with non-trivial Möbius function. If H is a maximal subgroup of L, then $\mu_L(H) = -1$. On the other hand $\mu_L(H) \neq 0$ only if H is an intersection of maximal subgroups of L. Now recall that if M is a maximal supplement to N in L, then there are two possibilities: either $M \cap N$ is a subdirect product of S^r (a maximal subgroup of diagonal type) or $M \cap N \cong U^r$ with $U < S$ (a maximal subgroup of product type); in the second case if $1 \neq U$, then there exists a maximal supplement Y of S in X such that M is conjugate to $(Y \wr \operatorname{Sym}(r)) \cap L$. We will say that n is a *useful index* of L if $b_n \neq 0$ and there exists a prime p which divides $|S|$ but does not divide n.

Lemma 2.1. *If n is a useful index of L, then there exists a subgroup Y of X such that $X = YS$ and $n = |X : Y|^r$.*

Proof. Since $b_n \neq 0$, there exists $H \leqslant L$ with $HN = L$, $|L : H| = n$ and $\mu_L(H) \neq 0$. In particular H must be an intersection of maximal subgroups of L and all of these maximal subgroups must be of product type, since otherwise $|S|$ would divide $|L : M|$ (and consequently n) for some maximal subgroup M containing H. At this point it is easy to check (see for example the proof of [2, Lemma 5]) that $H \cap N \cong (Y \cap S)^r$ for a suitable supplement Y of S in X.

Lemma 2.2. *Let u be a positive integer such that there exists a prime p which divides $|S|$ but does not divide u, and let $\mathscr{U}$ be the set of subgroups Y with index u in X and with the property that $YS = X$. If $\mathscr{U} \neq \varnothing$ and every subgroup of $\mathscr{U}$ is maximal, then u^r is a useful index of L and $b_{u^r} < 0$.*

Proof. By the same arguments of the previous lemma, all subgroups M of L with $MN = L$ and $|L : M| = u^r$ are maximal; moreover, by [2, Lemma 2], the set $\mathscr{M}$ of maximal subgroups of L with these properties is non-empty. Hence $b_{u^r} = -|\mathscr{M}| < 0$.

Given a prime q, we denote by $v_q(n)$ the largest integer r such that q^r divides n. If q divides $|S|$, we will say that a useful index n of L is *q-useful* if n is divisible by q.

Lemma 2.3. *Assume that L is monolithic primitive group with $\operatorname{soc} L = (\mathrm{Alt}(m))^r$ and that m is not a prime, and let q be the largest prime with $q \leqslant m$. Define w as follows:*

$$w = \begin{cases} \binom{m}{q-1} & \text{if } m \notin \{6, 10\}, \\ 126 & \text{if } m = 10, \\ 10 & \text{if } m = 6. \end{cases}$$

Then $b_{w^r} < 0$ and w^r is the smallest q-useful index in L.

Proof. First note there there exists a prime p which divides $|\mathrm{Alt}(m)|$ but does not divide w. Indeed we take $p = 3$ if $m = 6$, $p = 5$ if $m = 10$, while in the other cases there exists a prime p with $m/2 < p < q < m$ (e.g. by Nagura's result [9]). Note that either $m = 6$ or $X \in \{\mathrm{Alt}(m), \mathrm{Sym}(m)\}$. In any case, by Lemma 2.1 and Lemma 2.2, it suffices to prove that

(1) X contains a supplement Y of S with $|X : Y| = w$, and

(2) if U is a supplement of S in X with index $|X : U|$ at most w and a multiple of q, then $|X : U| = w$ and U is a maximal subgroup.

These statements can easily be verified when $m \in \{6, 10\}$, so assume that $m \neq 6, 10$. First note that given a subset $\Delta \subset \Omega = \{1, \ldots, m\}$ of size $|\Delta| = q - 1$, the subgroup $Y = (\mathrm{Sym}(\Delta) \times \mathrm{Sym}(\Omega \backslash \Delta)) \cap X$ is a maximal subgroup with index w in X. Now let

U be a supplement of S in X with index $x = |X : U|$, where q divides x and $x \leqslant w$. Since

$$x \leqslant w < \binom{m}{m-q+2}$$

and $m - q + 2 \leqslant m/2$, then by [4, Theorem 5.2 A, B] one of the following holds.

(a) There exists $\Delta \subseteq \{1, \ldots, m\}$ such that

$$|\Delta| = k < m - q + 2 \quad \text{and} \quad X_{(\Delta)} \leqslant U \leqslant X_{\{\Delta\}}.$$

Considering the indices we get that x, and hence q, divides $m!/(m-k)!$. Since $m/2 < q < m$, we have $v_q(m!) = 1$, so that $v_q((m-k)!) = 0$ and thus $m - k < q$. As $k < m - q + 2$ we conclude that $k = m - q + 1$; thus $x = w$ and $U = X_{\{\Delta\}}$ is maximal.

(b) m is even and U has index $x = \frac{1}{2}\binom{m}{m/2}$. When $m \geqslant 30$, Nagura's result [9] gives that $q > 5/6m$ and this implies that

$$x > \binom{m}{\lfloor 5/6m \rfloor - 1} \geqslant \binom{m}{q-1} = w.$$

It can be checked by direct computation that

$$x > \binom{m}{q-1} = w$$

even for $m < 30$, $m \notin \{6, 10\}$. This contradicts $x \leqslant w$.

(c) $m = 9$ or 8 and X has index 120, 15 or 30. Since none of these indices is divisible by $q = 7$, this case never occurs.

Lemma 2.4. *Assume that L is a monolithic primitive group with* $\operatorname{soc} L = (\operatorname{Alt}(m))^r$ *and* $m > 10$. *Let p, q be primes with $p < q < m$ and let α be the minimal useful index with the properties that $v_p(\alpha) = 0$ and $v_q(\alpha) = r$. If $\alpha < \binom{m}{q-1}^r$, then $b_\alpha < 0$.*

Proof. By Lemma 2.1 there exists a supplement Y to S in X with index w such that $\alpha = w^r$; clearly $v_p(w) = 0$, $v_q(w) = 1$ and $w < \binom{m}{q-1}$. Let z be the minimal index of a supplement to S in X with the properties that $v_p(z) = 0$ and $v_q(z) = 1$; then $z \leqslant w < \binom{m}{q-1}$. We claim that every supplement Y of S with index z in X is a maximal subgroup. Since $z < \binom{m}{q-1}$ and $m > 10$, we can apply [4, Theorem 5.2 A, B] which says that Y is either a maximal imprimitive subgroup, and we are finished, or Y lies between a maximal subgroup M with index $\binom{m}{k}$ and a subgroup of index $m!/(m-k)!$ where $k < \min\{q-1, m-q+1\}$. Note that, as q divides z, then $v_q(m!/(m-k)!) \geqslant 1$. If $q - 1 > m/2$, then $m < 2q$ and $v_q(m!) = 1$; since $k < m - q + 1$, we get that $m - k + 1 > q$ and hence q does not divide $m!/(m-k)!$, a contradiction; so this case never occurs. Therefore $q - 1 \leqslant m/2$. Then $k < q - 1 < q$ and q does not divide $k!$, and hence

$$v_q\left(\binom{m}{k}\right) = v_q(m!/(m-k)!) = 1.$$

Moreover, as $\binom{m}{k}$ divides z, we have $v_p\left(\binom{m}{k}\right) = 0$. By minimality of z, we have $z = \binom{m}{k}$ and $Y = M$ is a maximal subgroup, as claimed.

By Lemma 2.2 it follows that z^r is a useful index of L and $b_{z^r} < 0$; by minimality of α we conclude that $\alpha = z^r$ and $b_\alpha < 0$.

3 The number of non-isomorphic composition factors

Assume that G is a finitely generated profinite group, choose a descending series $\{G_i\}_{i \in \mathbb{N}}$ as described in Section 2 and assume that almost every composition factor is cyclic or isomorphic to an alternating group. Let $\pi(G)$ be the set of prime divisors of indices of open subgroups of G. The aim of this section is to prove that if the formal series $P_G(s) = \sum_n a_n/n^s$ is rational, then $\pi(G)$ is finite. We start by noting that if $P_G(s)$ is rational then the set π of primes p such that there exists n divisible by p with $a_n \neq 0$ is finite. Moreover we have:

Lemma 3.1. *Assume that $P_G(s)$ is rational and let p be a prime with $p \notin \pi$; then, for any $i \in I$, the following assertions hold.*

(1) *If G_i/G_{i+1} is a non-Frattini abelian chief factor, then $|G_i/G_{i+i}|$ is not a p-power.*

(2) *If G_i/G_{i+1} is non-abelian, then the almost simple group X_i has no maximal subgroups of p-power index which are supplements for $S_i = \operatorname{soc} X_i$ in X_i.*

Proof. We first note that G has no subgroup with index a power of a prime p. Indeed, if we consider the minimal p-power index, say p^t, of a subgroup of G, then every subgroup H with index p^t is definitely a maximal subgroup, so that $\mu_G(H) = -1$ and therefore the coefficient $a_{p^t} = \sum_{|G:H|=p^t} \mu_G(H)$ is non-zero, against the definition of π. If G_i/G_{i+1} is a non-Frattini chief factor of p-power order, then there is a complement to G_i/G_{i+1} in G/G_{i+1}, while if X_i is almost simple and contains a subgroup Y with $|X_i : Y| = p^t$ and $X_i = YS_i$, then if t is minimal, by [2, Lemma 2], L_i, and consequently G, has a maximal subgroup of index p^{tr_i}.

In the case of prosolvable groups, Lemma 3.1 leads immediately to the conclusion that $\pi(G)$ is finite if $P_G(s)$ is rational. The same is true also under our weaker hypothesis, but the argument is more complicated. We will need the following lemma.

Lemma 3.2. *Let $\mathcal{F}$ be a finite set of simple groups. Assume that, for any $i \in \mathbb{N}$, if $P_i(s) \neq 1$, then S_i is isomorphic to an element of $\mathcal{F}$. Then $\pi(G)$ is finite.*

Proof. Let $p \in \pi(G)$. Then p divides $|G_i/G_{i+1}|$ for an index $i \in \mathbb{N}$; let i be the minimal index with this property. If G_i/G_{i+1} is abelian, then $|G_i/G_{i+1}| = p^{r_i}$ and, by the Schur–Zassenhaus Theorem, G_i/G_{i+1} is a complemented chief factor. Since $P_i(s) = 1$

if and only if G_i/G_{i+1} is a Frattini chief factor, it follows that p is a prime divisor of $|S|$ for some $S \in \mathscr{F}$. Therefore $\pi(G)$ is finite.

Proposition 3.3. *Let G be a finitely generated profinite group such that almost every composition factor is cyclic or isomorphic to an alternating group. If $P_G(s)$ is rational then $\pi(G)$ is finite.*

Proof. Using the notation introduced in Section 2, we have

$$P_G(s) = \sum_n a_n/n^s = \prod_{i \in \mathbb{N}} P_i(s),$$

where $P_i(s)$ is the finite Dirichlet series associated to the chief factor G_i/G_{i+1}. Let I be the set of indices such that either S_i is cyclic of order n_i or $S_i \cong \mathrm{Alt}(n_i)$ is an alternating group and such that $P_i(s) \neq 1$. Since all but a finite number of composition factors are abelian or alternating groups, if we restrict the product to the subset I, we still get that $Q(s) = \sum_n c_n/n^s = \prod_{i \in I} P_i(s)$ is rational. In particular, we can choose a prime number $u > 10$ such that $a_n = c_n = 0$ whenever n is divisible by a prime $q \geqslant u$. Our goal is to prove that $n_i < u$ for every $i \in I$; from this and Lemma 3.2 it follows that $\pi(G)$ is finite. Assume for a contradiction that the set

$$I_u = \{i \in I \mid n_i \geqslant u\}$$

is non-empty. By Lemma 3.1, for each $i \in I_u$, the number n_i is not a prime and S_i is of alternating type; that is, $S_i \cong \mathrm{Alt}(n_i)$. Now we define

$$r = \min\{r_i \mid n_i \geqslant u\} = \min\{r_i \mid i \in I_u\},$$
$$m = \min\{n_i \mid r_i = r, i \in I_u\};$$

as $u > 10$, we can choose two primes p and q such that $m/2 < p < q \leqslant m$ and q is the largest prime not greater then m; note that m is not prime, so that $q \neq m$, and that $u \leqslant q$. Now consider the set Λ of all integers n divisible by q but not by p. If $n \in \Lambda$ and $b_{i,n} \neq 0$, then $n_i \geqslant q > p$, so $i \in I_u$ and n is a useful index for L_i; hence, by Lemma 2.1, n is an r_ith power and $v_q(n) \geqslant r$. Moreover if i is an index of I_u such that $m = n_i$ and $r = r_i$, then, by Lemma 2.3, $v = \binom{m}{q-1} \in \Lambda$ and $b_{i,v^r} < 0$. Choose $\alpha \in \Lambda$ minimal with the properties that there exist $i \in I_u$ such that $r_i = r$, $v_q(\alpha) = r$ and α is a useful index for L_i: then $\alpha \leqslant v^r$. Note that if $n \in \Lambda$ is a useful index for L_i, then either $v_q(n) > r$ or $r_i = r$, $v_q(n) = r$ and $n \geqslant \alpha$. This implies in particular that the coefficient c_α of $1/\alpha^s$ in $Q(s) = \prod_{i \in I} P_i(s)$ is

$$c_\alpha = \sum_{i \in I_u, r_i = r} b_{i,\alpha}.$$

If $r = r_i$ and $m = n_i$, then v^r is the minimal q-useful index for L_i and thus $b_{i,\alpha} \leqslant 0$. Now let $i \in I_u$ with $r_i = r$, $n_i \neq m$ and assume that $b_{i,\alpha} \neq 0$. Since $n_i > m$ we get

$$\alpha \leqslant \binom{m}{q-1}^r < \binom{n_i}{q-1}^r,$$

and we conclude by Lemma 2.4 that $b_{i,\alpha} < 0$. Since $b_{i,\alpha} \neq 0$ for at least one index i, this gives that $c_\alpha = \sum_i b_{i,\alpha} \neq 0$. But q divides α and $q \geqslant u$, and this contradicts the choice of u.

4 Infinite products of formal Dirichlet series

Let $\mathscr{R}$ be the ring of formal Dirichlet series with integer coefficients. For every prime number p we consider the ring endomorphism of $\mathscr{R}$ defined by

$$F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \mapsto F^p(s) = \sum_{(n,p)=1} \frac{a_n}{n^s}.$$

The following observation is crucial for the proof that if G is prosoluble and $P_G(s)$ is rational, then $G/\mathrm{Frat}(G)$ is finite:

Lemma 4.1. *Let p be a prime and $\{F_i(s)\}_{i\in I}$ be a family of finite Dirichlet series. If $\prod_{i\in I} F_i(s)$ is rational, then $\prod_{i\in I} F_i^p(s)$ is rational.*

Note that if the chief factor G_i/G_{i+1} is abelian, then the Dirichlet series $P_i(s)$ is very simple: $P_i(s) \neq 1$ if and only if G_i/G_{i+1} is non-Frattini; in particular if $|G_i/G_{i+1}| = p_i^{r_i}$, then

$$P_i(s) = 1 - \frac{c_i}{(p_i^{r_i})^s}$$

where c_i is the number of complements of G_i/G_{i+1} in G/G_{i+1}. When G is prosoluble, we consider the set I_p of the indices $i \in I$ such that G_i/G_{i+1} is non-Frattini and has order a p-power: $P_G(s)$ is the product of the Euler factors

$$E_p(s) = \prod_{i\in I_p} \left(1 - \frac{c_i}{(p^{r_i})^s}\right)$$

where p runs through the set of primes. If $P_G(s)$ is rational, then, by Proposition 3.3 and Lemma 4.1, every Euler factor $E_p(s)$ is rational and $E_p(s) = 1$ for all but a finite number of primes p. So, in the solvable case, it was sufficient to work on the Euler factors, proving that if $E_p(s) = \prod_{i\in I_p} P_i(s)$ is rational, then the set I_p is finite. We succeeded in proving this, thanks to the following consequence of the Skolem–Mahler–Lech Theorem:

Proposition 4.2 ([3, Proposition 3.2]). *Let $I \subseteq \mathbb{N}$ and let q, r_i, c_i, be positive integers for each $i \in I$. Assume that the product*

$$F(s) = \prod_{i \in I} \left(1 - \frac{c_i}{(q^{r_i})^s}\right)$$

is rational and that there exists a prime t such that t does not divide r_i for any $i \in I$. Then I is finite.

The earlier approach fails in the general case, since the finite series $P_i(s)$ are more complicated and may involve many non-trivial terms. However we will be able to prove that if the product $P_G(s) = \prod_{i \in I} P_i(s)$ is rational, then it is possible to construct nice subseries $P_i^*(s)$ of $P_i(s)$ (all of the kind $1 + \gamma_i/w^{r_i s}$ for a fixed w), such that the product $\prod_{i \in I} P_i^*(s)$ is still rational and satisfies the assumption of Proposition 4.2. The technical result we will employ in order to do this is the following:

Proposition 4.3. *Let $F(s)$ be a product of finite Dirichlet series*:

$$F(s) = \prod_{i \in I} F_i(s), \quad \text{where } F_i(s) = \sum_{n \in \mathbb{N}} \frac{b_{i,n}}{n^s}.$$

Let q be a prime and Λ the set of positive integers divisible by q. Assume that there exists a set $\{r_i\}_{i \in I}$ of positive integers such that if $n \in \Lambda$ and $b_{i,n} \neq 0$ then n is an r_i-th power of some integer and $v_q(n) = r_i$. Define

$$w = \min\{x \in \mathbb{N} \mid v_q(x) = 1 \text{ and } b_{i,x^{r_i}} \neq 0 \text{ for some } i \in I\}.$$

If $F(s)$ is rational, then the product

$$F^*(s) = \prod_{i \in I} \left(1 + \frac{b_{i,w^{r_i}}}{(w^{r_i})^s}\right)$$

is rational.

Proof. Observe that in the product

$$F(s) = \prod_{i \in I} F_i(s) = \sum_{n \in \mathbb{N}} \frac{c_n}{n^s}$$

each integer n such that $c_n \neq 0$ satisfies $n \geqslant w^{v_q(n)}$. Moreover for $n = w^{v_q(n)}$ the coefficient c_n of $F(s)$ is in fact the coefficient of $1/n^s$ in the product $F^*(s)$:

$$F^*(s) = \prod_{i \in I} \left(1 + \frac{b_{i,w^{r_i}}}{(w^{r_i})^s}\right) = \sum_{t \in \mathbb{N}} \frac{c_{w^t}}{(w^t)^s};$$

this means that we are able to recognize the powers of $1/w^s$, and hence $F^*(s)$, as a subseries of $F(s)$.

Let $F(s)$ be rational and let $A(s)$ be a finite Dirichlet series such that $A(s)F(s)$ is a finite Dirichlet series. Let

$$A(s) = \sum \frac{a_n}{n^s};$$

we set

$$\xi = \min\{x \in \mathbb{Q} \mid x = n/w^{v_q(n)} \text{ and } a_n \neq 0\}$$

and

$$\mathcal{N} = \{n \in \mathbb{N} \mid n/w^{v_q(n)} = \xi \text{ and } a_n \neq 0\} = \{\xi w^m \in \mathbb{N} \mid a_{\xi w^m} \neq 0, m \in \mathbb{N}\}.$$

Finally we define the new series

$$A^*(s) = \sum_{n \in \mathcal{N}} \frac{a_n}{n^s} = \sum_m \frac{a_{\xi w^m}}{(\xi w^m)^s}.$$

We now prove that $A^*(s)F^*(s)$ is a finite Dirichlet series, from which it follows that $F^*(s)$ is rational.

Note that

$$A^*(s)F^*(s) = \sum_{\substack{\xi w^m \in \mathcal{N} \\ t \in \mathbb{N}}} \frac{a_{\xi w^m} c_{w^t}}{(\xi w^{(m+t)})^s}.$$

We examine the coefficient of $1/(\xi w^{(m+t)})^s$ in $A(s)F(s)$: this is the sum

$$\sum_{ln = \xi w^{(m+t)}} a_l c_n \quad \text{where } l \in \mathbb{N},\ n \geqslant w^{v_q(n)}.$$

Take l and n such that $a_l c_n \neq 0$ and $ln = \xi w^{(m+t)}$. If $n > w^{v_q(n)}$ then

$$\xi w^{(m+t)} = ln > l w^{v_q(n)}$$

and, since $v_q(n) + v_q(l) = m + t$, this gives $l/w^{v_q(l)} < \xi$, a contradiction. Hence $n = w^{v_q(n)}$ and c_n/n^s is a term of $F^*(s)$. Moreover

$$\xi w^{(m+t)} = nl = w^{v_q(n)} l$$

implies $l/w^{v_q(l)} = \xi$ and hence $l \in \mathcal{N}$. This means that the coefficient of $1/(\xi w^{(m+t)})^s$ in $A(s)F(s)$ is the coefficient of $1/(\xi w^{(m+t)})^s$ in $A^*(s)F^*(s)$, and since $A(s)F(s)$ is a finite series, we conclude that $A^*(s)F^*(s)$ is finite, too.

5 Chief factors

In this section we will prove that given a finitely generated profinite group G with $\pi(G)$ finite, there exists a prime t such that for every primitive monolithic image L of G, t does not divide the composition length r of $\operatorname{soc} L = S^r$, where S is a simple group.

Let π be a finite set of primes and let $\mathscr{S}$ be the set of finite simple groups S such that $\pi(S) \subseteq \pi$; by the classification of finite simple groups $\mathscr{S}$ is finite. Now let $\mathscr{Q}$ be the set of quasisimple groups X such that $X/Z(X) \in \mathscr{S}$; since the universal cover of a finite non-abelian simple group is finite, it follows that the set $\mathscr{Q}$ is finite. Then, for every prime p, define α_p to be the largest prime divisor of the degree of an absolutely irreducible $\mathbb{F}_p X$-module, for $X \in \mathscr{Q}$. Finally we set

$$\eta = \max(\{\alpha_p\}_{p \in \pi} \cup \pi).$$

Lemma 5.1. *Let H be a finite π-group. Let n be the degree of an irreducible linear representation over a finite field F of the group H. If q is a prime divisor of n, then $q \leqslant \eta$.*

Proof. By a result of Brauer there exists a field extension L of F such that L is a splitting field for H and all of its subgroups, and the degree $|L : F|$ divides $\varphi(\exp(H))$. Let V be an irreducible FH-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 divides $\varphi(\exp(H))$; if $\pi(H) = \{p_1, \dots, p_r\}$ and $\exp(H) = p_1^{m_1} \dots p_r^{m_r}$, then

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

It follows that each prime divisor of r, dividing $\varphi(\exp(H))$, is bounded by $\max\{\pi(H)\} \subseteq \max\{\pi\}$; this implies that we may assume that $F = L$ or, equivalently, that without loss of generality F is algebraically closed.

We shall prove the lemma by induction on $|H|$. If V is an imprimitive FH-module, say $V = W^t$, then H has a transitive representation with degree t, for a π-number t, and W is an FK-irreducible module where $K = N_H(W)$; since $n = t \cdot \dim W$, a prime divisor q of n divides either t, whence $q \in \pi$, or $q \leqslant \eta$, by the inductive assumption.

So we can assume that H is an absolutely irreducible primitive group. Then there are primitive groups $H_i \leqslant \mathrm{GL}(n_i, F)$ where $n = n_1 \dots n_r$ such that $Z_i = Z(H_i) \cong F^*$, each H_i/Z_i is a homomorphic image of H (hence a π-group) and every normal subgroup of H_i is scalar or irreducible (see e.g. [10, §II 2.3]). Thus we are reduced to proving that each prime divisor q of n_i is bounded by η.

If H_i contains a non-scalar soluble normal subgroup, then we choose A to be minimal with this property: we conclude that A is an r-group for a prime r and n_i is a power of r, so that $r \in \pi$ and n_i is a π-number.

Otherwise, if all soluble normal subgroups of G are scalar, we choose a minimal normal subgroup N/Z_i of H_i/Z_i; then N' is an irreducible normal subgroup with degree n_i and is the central product of $Q_1, \dots, Q_s$ for some $Q_i \in \mathcal{Q}$; thus $n_i = k_1 \dots k_s$ where k_i is the degree of an absolutely irreducible representation of Q_i, and therefore each prime divisor of k_i is bounded by α_p.

Corollary 5.2. *Let G be a finitely generated profinite group. If $\pi(G)$ is finite, then there exists a prime t such that, for every $i \in I$, the composition length r_i of the chief factor G_i/G_{i+1} is not divisible by t.*

Proof. Let u be a prime divisor of r_i where $G_i/G_{i+1} \cong S_i^{r_i}$. If S_i is abelian, then Proposition 5.1 gives $u \leqslant \eta$; otherwise $\operatorname{soc} L_i = S_i^{r_i}$ where S is a finite non-abelian group and r_i is the degree of a transitive representation of a finite image of G, so that $u \in \pi(G)$.

6 The main theorem

Theorem 6.1. *Let G be a finitely generated profinite group such that almost every composition factor is cyclic or isomorphic to an alternating group. Then $P_G(s)$ is rational only if G has finitely many non-Frattini chief factors, i.e. only if $G/\mathrm{Frat}(G)$ is a finite group.*

Proof. Let us use the notation introduced in Section 2 and let I^* be the set of indices such that $P_i(s) \neq 1$ and S_i is either cyclic of order n_i or isomorphic to $\mathrm{Alt}(n_i)$. If $P_G(s)$ is rational, then clearly also $\prod_{i \in I^*} P_i(s)$ is rational. Moreover, if for a given integer n the set $\{i \in I^* \mid n_i = n\}$ is finite, then the product

$$\prod_{\substack{i \in I^* \\ n_i \neq n}} P_i(s)$$

is again rational. Define J to be the subset of I^* of the indices i with the property that $n_i = n_j$ for infinitely many $j \in I^*$; since by Proposition 3.3 there is a bound on the set $\{n_i\}_{i \in I^*}$, the set J differs from I^* for a finite number of indices and thus the product

$$\prod_{i \in J} P_i(s)$$

is still rational. Our claim is that J is empty; this will imply that there are only finitely many non-Frattini chief factors and consequently that $G/\mathrm{Frat}(G)$ is a finite group (see e.g. [3, Theorem 4.3]). Assume by contradiction that J is non-empty and set

$$\begin{aligned} m_0 &= \max\{n_i \mid i \in J\}, \\ q &= \text{largest prime} \leqslant m_0, \\ m &= \min\{n_i \mid n_i \geqslant q, i \in J\}, \\ p &= \text{largest prime} < q. \end{aligned}$$

We will work on the product $\prod_{i \in J} P_i^p(s)$ of the finite Dirichlet series

$$P_i^p(s) = \sum_{p \nmid n} \frac{b_{i,n}}{n^s}.$$

Since $\prod_i P_i(s)$ is rational, then also $\prod_i P_i^p(s)$ is rational (see Corollary 4.1). Let Λ be the set of positive integers n divisible by q but not by p. Note that for any choices of i, if $n \in \Lambda$ and $b_{i,n} \neq 0$, then $n_i \geqslant q > p$ and, by Lemma 2.1, there exists a subgroup Y_i of index x_i in X_i such that $n = x_i^{r_i}$; hence $v_q(n) = r_i v_q(x_i)$. On the other hand, $q > m_0/2$ implies that $n_i < 2q$, which means that $v_q(x_i) \leqslant 1$ and thus $v_q(n) = r_i$. Let

$$w = \min\{x \in \Lambda \mid b_{i,x^{r_i}} \neq 0 \text{ and } v_q(x) = 1\}.$$

By Proposition 4.3 applied to $\prod_i P_i^p(s)$, it follows that the product

$$\prod_{i \in J} \left(1 + \frac{b_{i,w^{r_i}}}{w^{r_i \cdot s}}\right)$$

is rational. By Proposition 3.3 we have that $\pi(G)$ is finite, and hence, by Corollary 5.2, there exists a prime t such that t does not divide r_i for every $i \in J$. Now it is sufficient to prove that $b_{i,w^{r_i}} \leqslant 0$ for every $i \in J$ and $b_{i,w^{r_i}} < 0$ for infinitely many $i \in J$ to reach a contradiction and prove the theorem; indeed by the Skolem–Mahler–Lech Theorem (Proposition 4.2) it follows that if $b_{i,w^{r_i}} \leqslant 0$ for every $i \in J$, then $b_{i,w^{r_i}} = 0$ for all but a finite number of indices $i \in J$.

We have two possibilities:

Case 1: $m = q$. If $b_{i,q^{r_i}} \neq 0$ then X_i has a subgroup of index q and therefore i is one of the infinitely many indices of J such that $n_i = m = q$. If S_i is abelian then $b_{i,q^{r_i}} < 0$; otherwise $S_i = \mathrm{Alt}(q)$ and every supplement with index q is maximal, so that $b_{i,q^{r_i}} < 0$ by Lemma 2.2. It follows that $w = q$ and $b_{i,w^{r_i}} < 0$ for infinitely many $i \in J$.

Case 2: $m > q$. In this case, both m_0 and m are non-prime, since otherwise we would have $m_0 = q = m$ or $m = q$. Moreover, if $n \in \Lambda$ and $b_{i,n} \neq 0$, then $n_i \geqslant q$ hence $n_i \geqslant m > q$; in particular S_i is non-abelian, for otherwise $n = q^{r_i}$ and $n_i = q$. We claim that

$$w = \begin{cases} \binom{m}{q-1} & \text{if } m \notin \{6, 10\}, \\ 126 & \text{if } m = 10, \\ 10 & \text{if } m = 6, \end{cases}$$

and $b_{i,w^{r_i}} \leqslant 0$ for every $i \in J$. Whenever $n_i = m$ (and this holds for infinitely many $i \in J$), by Lemma 2.3 the number w^r is the smallest q-useful index in L_i and $b_{i,w^{r_i}} < 0$. For $n_i < m$ there are no q-useful indices, so let $n_i > m$. As q is still the largest prime less than or equal to n_i, and n_i is not a prime, we can apply Lemma 2.3. If $n_i \notin \{6, 10\}$, then the minimal q-useful index in L_i prime to p is

$$\binom{n_i}{q-1}^{r_i} > \binom{m}{q-1}^{r_i} = w^{r_i}$$

since $n_i > m$. We cannot have $n_i = 6$ since then $n_i = m$, and so the last cases are $n_i = 10$ and $m = 8$ or $m = 9$; the minimal q-useful index in L_i is then 126^{r_i} which is larger than $\binom{m}{q-1}^{r_i}$ for both $m = 8, 9$ (with $q = 7$). This proves that $b_{i,w^{r_i}} \leqslant 0$, and so our discussion is complete.

References

[1] E. Detomi and A. Lucchini. Crowns in profinite groups and applications. In *Noncommutative algebra and geometry*, Lecture Notes in Pure Appl. Math. 243 (Chapman & Hall/CRC, 2006), pp. 47–62.

[2] E. Detomi and A. Lucchini. Profinite groups with multiplicative probabilistic zeta function. *J. London Math. Soc.* (2) **70** (2004), 165–181.

[3] E. Detomi and A. Lucchini. Profinite groups with a rational probabilistic zeta function. *J. Group Theory* **9** (2006), 203–217.

[4] J. Dixon and B. Mortimer. *Permutation groups*. Graduate Texts in Math. 163 (Springer-Verlag, 1996).

[5] P. Hall. The Eulerian functions of a group. *Quart. J. Math. Oxford Ser.* (2) **7** (1936), 134–151.

[6] A. Lubotzky and D. Segal. *Subgroup growth*. Progress in Math. 212 (Birkhäuser Verlag, 2003).

[7] A. Mann. A probabilistic zeta function for arithmetic groups. *Internat. J. Algebra Comput* **15** (2005), 1053–1059.

[8] A. Mann. Positively finitely generated groups. *Forum Math.* **8** (1996), 429–459.

[9] J. Nagura. On the interval containing at least one prime number. *Proc. Japan Acad.* **28** (1952), 177–181.

[10] A. E. Zalesskij. Linear groups. In *Algebra, IV*, Encyclopaedia Math. Sci. 37 (Springer-Verlag, 1993), pp. 97–196.

Received 28 April, 2006; revised 14 September, 2006

Eloisa Detomi, Dipartimento di Matematica Pura ed Applicata, Università di Padova, via Trieste, 63, 35121 Padova, Italy
E-mail: detomi@math.unipd.it

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