# Chapter 2

# Preliminary results

## 2.1 Factorization of $P_G(s)$

Let $G$ be a finitely generated profinite group. We associate to $G$ the formal Dirichlet series

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

Here $\mu_G$ is the Möbius function defined on the lattice of open subgroups of $G$ recursively by $\mu_G(G) = 1$ and $\mu_G(H) = -\sum_{H<K\leq G} \mu_G(K)$ if $H < G$. Since $G$ is finitely generated, $G$ has only finitely many subgroups of finite index $n$ for each $n$ (see [Hal50, Section 2]), and so $a_n$ is well-defined for each $n$. Moreover, Nikolov and Segal showed in [NS07] that each subgroup of finite index in $G$ is open.

Given a closed normal subgroup $N$ of $G$, we define a formal Dirichlet series $P_{G,N}(s)$ as follows:

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

Notice that $P_G(s) = P_{G,G}(s)$. Moreover, $N$ admits a supplement in $G$ if and only if it is not contained in the Frattini subgroup of $G$. It follows easily that $P_{G,N}(s) = 1$ if and only if $N \leq \mathrm{Frat}(G)$.

When $G$ is a finite group, we have a factorization (see [Bro00, Section 2.2])

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

We have a similar result for the group $G$ in our context. Recall that the *convolution product*

of two formal Dirichlet series $A(s) = \sum_n a_n/n^s$ and $B(s) = \sum_n b_n/n^s$, denoted by $A(s) * B(s)$, is the Dirichlet series $\sum_n c_n/n^s$ with $c_n = \sum_{d|n} a_d b_{n/d}$.

**Theorem 2.1.1** ([DL06b, Theorem 13])**.** *If $G$ is finitely generated profinite group and $N$ is a closed normal subgroup of $G$ then $P_G(s) = P_{G/N}(s) * P_{G,N}(s)$.*

*Proof.* Let $n \in \mathbb{N}$. We need to prove that the coefficients of $1/n^s$ in $P_G(s)$ and $P_{G/N}(s) * P_{G,N}(s)$ are equal, that is

$$\sum_{|G:H|=n} \mu_G(H) = \sum_{d|n} \left( \sum_{\substack{N<H_1<G \\ |G:H_1|=d}} \mu_G(H_1) \right) \left( \sum_{\substack{H_2N=G \\ |G:H_2|=n/d}} \mu_G(H_2) \right). \tag{2.1}$$

Let $N_k$ be the intersection of the open subgroups of $G$ of index $k$. Then $N_k$ has finite index in $G$ since

$$|G : N_k| \leq \prod_{|G:H|=k} |G : H|.$$

Let $X_n$ be the intersection of the open subgroups of $G$ of index at most $n$, i.e, $X_n = \bigcap_{k=1}^{n} N_k$, then $X_n$ is characteristic, and hence normal, in $G$. Since $G$ is finitely generated, $X_n$ is a finite intersection (see [Hal50, Section 2]), thus $X_n$ is open. We have from [Bro00, Section 2.2] that

$$P_{G/X_n}(s) = P_{G/NX_n}(s) * P_{G/X_n, NX_n/X_n}(s). \tag{2.2}$$

If $|G : H| \leq n$ then $X_n \leq H$ and $\mu_G(H) = \mu_{G/X_n}(H/X_n)$. So it follows from (2.2) that the terms in (2.1) are equal to the coefficients of $1/n^s$ in the two series in (2.2). □

When $G$ is a finite group with a chief series

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = 1$$

then by iterating the above formula, we obtain a factorization of $P_G(s)$ as

$$P_G(s) = \prod_{i=0}^{n-1} P_{G/G_{i+1}, G_i/G_{i+1}}(s).$$

In order to obtain such a result for finitely generated profinite groups, we first define a chief factor in a profinite group and an equivalence relation between chief factors.

We say that a section $H/K$ is a *chief factor* of a profinite group $G$ if $H$ and $K$ are closed normal subgroups of $G$ with $K < H$ and for any closed normal subgroup $X$ of $G$ with $K \leq X \leq H$, either $X = K$ or $X = H$. Notice that if $H/K$ is a chief factor of $G$, then there is an open normal subgroup $N$ of $G$ such that $H/K \cong_G HN/KN$. Indeed, $H$ (as well as $K$) is the intersection of all open normal subgroups that contain it and so, as $H \neq K$, $HN \neq KN$ for at least one open normal subgroup $N$ of $G$. This implies that a chief factor $H/K$ is finite and that the action of $G$ on $H/K$ is irreducible and continuous.

A chief factor $H/K$ is called *Frattini* if $H/K \leq \mathrm{Frat}(G/K)$. Notice that if $H/K$ is a Frattini factor, then $HN/KN$ is Frattini for every closed normal subgroup $N$ of $G$. In particular, by considering a finite image of $G$, we find that a Frattini chief factor is abelian.

**Definition 2.1.2.** *Let $G$ be a profinite group and let $A$ and $B$ be two finite irreducible $G$-groups. We say that they are $G$-equivalent and put $A \sim_G B$, if there are two continuous isomorphisms $\phi : A \to B$ and $\Phi : A \rtimes G \to B \rtimes G$ such that the following diagram commutes:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & A \rtimes G & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \Phi} & & \| & & \\ 1 & \longrightarrow & B & \longrightarrow & B \rtimes G & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

It is clear that this is an equivalence relation. A group isomorphism $\phi : A \to B$ is called $G$-isomorphic if $(x^g)^\phi = (x^\phi)^g$. If $\phi$ is $G$-isomorphic then $(ag)^\Phi = a^\phi g, a \in A, g \in G$, defines an ismorphism $\Phi : A \rtimes G \to B \rtimes G$ which makes the above diagram commutative. Hence two $G$-isomorphic $G$-groups are $G$-equivalent. Conversely, if $A$ and $B$ are abelian and $G$-equivalent then $A$ and $B$ are $G$-isomorphic : for any $g \in G$ there exists an element $b_g \in B$ such that $g^\Phi = b_g g$, so for any $a \in A$ we have $(a^g)^\phi = (a^g)^\Phi = (a^\Phi)^{g^\Phi} = (a^\phi)^{b_g g} = (a^\phi)^g$. However, for nonabelian $G$-groups, $G$-equivalence is strictly weaker than $G$-isomorphism. For example, the two minimal normal subgroups of $G = \mathrm{Alt}(5)^2$ are $G$-equivalent without being $G$-isomorphic.

Recall that a finite group $L$ is said to be *primitive* if it has a maximal subgroup such that its normal core $\bigcap_{x \in L} M^x$ is trivial. The socle $\mathrm{soc}(L)$ of a primitive group $L$ can be either an abelian minimal normal subgroup (I), or a nonabelian minimal normal subgroup (II), or the product of two nonabelian minimal normal subgroups (III) (see [BBE06, Theorem 1.1.7]). We say that $L$ is *primitive of type* I, II, III, respectively, and in the first two cases, we say that $L$ is *monolithic*.

As in the case of finite groups (see [DL03a]), the $G$-equivalence relation on chief factors of $G$ is related to the primitive epimorphic images of $G$:

**Lemma 2.1.3** ([DL04b, Lemma 3] )**.** *Let $G$ be a profinite group. Two chief factors $A$ and $B$ are $G$-equivalent as $G$-groups if and only if either they are $G$-isomorphic or there exists an open normal subgroup $N$ of $G$ such that $G/N$ is a primitive monolithic group of type III and the two minimal normal subgroups of $G/N$ are $G$-isomorphic to $A$ and $B$ respectively.*

Recall from [RZ10, Corollary 2.6.5] that any profinite group $G$ has a chain of closed normal subgroups

$$G_\mu = 1 \leq \cdots \leq G_0 = G$$

indexed by the ordinals $\lambda \leq \mu$ such that

- $G_\lambda / G_{\lambda+1}$ is a chief factor of $G$ for each $\lambda < \mu$,
- if $\lambda$ is a limit ordinal then $G_\lambda = \bigcap_{\nu<\lambda} G_\nu$.

Such a chain will be called *chief series* of $G$. If $G$ is countably based, in particular, if $G$ is a finitely generated profinite group, then $G$ has a chief series $\sum$ of length $\aleph_0$ (see [RZ10, Corollary 2.6.6])

$$\sum : G = G_0 \geq \cdots \geq G_i \geq \cdots \geq G_{\aleph_0} = 1. \tag{2.3}$$

For any irreducible $G$-group $A$, let $\delta_G(A)$ be the number of factors $G_i/G_{i+1}$ in the series $\sum$ which are non-Frattini and $G$-equivalent to $A$. Then $\delta_G(A)$ is independent on the chief series. Moreover, we have the following.

**Theorem 2.1.4** ([DL04b, Theorem 12])**.** *If $G$ is finitely generated then $\delta_G(A)$ is finite for every finite irreducible $G$-group $A$.*

Let $A$ be an irreducible $G$-group and let $\rho : G \to \mathrm{Aut}(A)$ be defined by $g \mapsto g^\rho$, where $g^\rho : a \mapsto a^g$ for all $a \in A$. The *monolithic primitive group associated with $A$* is defined as

$$L_A = \begin{cases} G^\rho A \cong A \rtimes G/C_G(A) & \text{if } A \text{ is abelian} \\ G^\rho \cong G/C_G(A) & \text{otherwise.} \end{cases}$$

Observe that $L_A$ is a finite primitive group of type I or II, and $\mathrm{soc}(L_A) \cong A$. Note that two $G$-equivalent $G$-groups may have different centralizers in $G$, but their associated monolithic primitive groups are isomorphic.

Let $L_A$ now be a finite monolithic primitive group, and let $A$ be its socle. We define

$$\begin{aligned} \widetilde{P}_{L_A,1}(s) &= P_{L_A,A}(s) \\ \widetilde{P}_{L_A,i}(s) &= P_{L_A,A}(s) - \frac{(1+q+\cdots+q^{i-2})\gamma}{|A|^s} \end{aligned} \tag{2.4}$$

where $\gamma = |C_{\mathrm{Aut}(A)}(L_A/A)|$ and $q = |\mathrm{End}_{L_A}(A)|$ if $A$ is abelian, $q = 1$ otherwise. In [DL03a, Theorem 17], it was shown that if $G$ is finite then the factors of $P_G(s)$ corresponding to the non-Frattini factors in a chief series are all of the kind $\widetilde{P}_{L_A,i}(s)$ for suitable choices of $L_A$ and $i$. We will prove that the same result also holds when $G$ is a finitely generated profinite group.

For any integer $n$, define $X_n$ to be the intersection of the open subgroups $H$ of $G$ with $|G:H| \leq n$. As we have seen above, $X_n$ is an open normal subgroup of $G$. In addition $\bigcap_n X_n = 1$, so we may produce a chief series $\sum$ by refining the series $\{X_n\}_{n\in\mathbb{N}}$.

Now fix an integer $m$. Let $H/K$ be a non-Frattini chief factor in $\sum$ and $P_{G/K,H/K}(s) = \sum_n \beta_n/n^s$. If $\beta_n \neq 0$ for some $1 \neq n \leq m$, then there exists an open subgroup $Y/K$ of $G/K$ with $G = YH$ and $|G:Y| = n$. This implies that $X_n \leq K$ since otherwise $H \leq X_n$, and as $X_n \leq Y$ we have that $G = HY = Y$, a contradiction. Thus $X_m \leq X_n \leq K$. As $G/X_m$ is finite, the set $\Omega_m$ of non-Frattini chief factors $H/K$ in $\sum$ with $X_m \leq K$ is finite. Then the following product

$$Q_m(s) = \prod_{H/K\in\Omega_m} P_{G/K,H/K}(s)$$

is a well-defined and finite Dirichlet series, say $Q_m(s) = \sum_n \alpha_{n,m}/n^s$. We define the *(infinite) convolution product* of the $\{P_{G/K,H/K}(s)\}$, where the $H/K$ are non-Frattini chief factors in $\sum$, to be

$$P_{\sum}(s) = \sum_n \frac{c_n}{n^s} \quad \text{where } c_1 = 1 \text{ and } c_n = \alpha_{n,n} \text{ for } n > 1.$$

Since $G$ is a finitely generated group, we have for every non-Frattini chief factor $A = H/K$ that $P_{G/K,H/K}(s) = \widetilde{P}_{L_A,i}(s)$ where $i = \delta_{G/K}(A)$ (see [DL06b, Theorem 15]). Hence the definition of $P_{\sum}(s)$ is independent on the choice of chief series of $G$.

Note that $Q_m(s) = P_{G/X_m}(s)$, thus by definition of $X_m$, the coefficient $a_m$ of $P_G(s) = \sum_m a_m/m^s$ is

$$a_m = \sum_{|G:X|=m} \mu_G(X) = \sum_{|G/X_m:X/X_m|=m} \mu_{G/X_m}(X/X_m) = \alpha_{m,m}$$

and so $a_m = c_m$. Since this holds for every integer $m$, we conclude that $P_G(s) = P_{\sum}(s)$. Therefore, we have proved the following.

**Theorem 2.1.5** ([DL06b, Theorem 17]). *Let $G$ be a finitely generated profinite group. Then*

$$P_G(s) = \prod_A \prod_{1 \leq i \leq \delta_G(A)} \widetilde{P}_{L_A,i}(s) \tag{2.5}$$

*where $A$ runs over the set of irreducible $G$-groups $G$-equivalent to a non-Frattini chief factor of $G$, and $L_A$ is the monolithic primitive group associated with $A$. Moreover, for every chief series $\sum$, the factorization of $P_G(s)$ corresponding to the non-Frattini factors in a chief series $\sum$ of $G$ is precisely (2.5).*

So from now we fix a countable descending series of open normal subgroups $\{G_i\}_{i\in\mathbb{N}}$ 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 $G$. Let $J$ be the set of indices $i$ with $G_i/G_{i+1}$ non-Frattini. For each $i \in J$, 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 Theorem 2.1.5, for each $i \in J$, a finite Dirichlet series $P_i(s) \neq 1$ is associated with the chief factor $G_i/G_{i+1}$, where $P_i(s) = \widetilde{P}_{L_A,j}(s)$ with $A \cong_G G_i/G_{i+1}$ and $j = \delta_{G/G_{i+1}}(G_i/G_{i+1})$. Therefore, $P_G(s)$ can be written as an infinite formal product of the finite Dirichlet series $P_i(s)$:

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

## 2.2 The probabilistic zeta function of a primitive monolithic group

Let $A/B$ be a nonabelian chief factor of a profinite group $G$ and let $L = G/C_G(A/B)$ be the monolithic primitive group associated with $A/B$. Note that the normal socle of $L$ is $N \cong A/B$. Consider the series

$$P_{L,N}(s) = \sum_n \frac{b_n}{n^s}, \quad \text{where } b_n = \sum_{\substack{|L:H|=n \\ L=HN}} \mu_L(H).$$

By definition, if $b_n \neq 0$ then $L$ contains a subgroup $H$ of index $n$ supplementing $N$ in $L$ and $\mu_L(H) \neq 0$. By [Hal36, Theorem 2.3], the second condition implies that $H$ is an inter-

section of maximal subgroups of $L$. In this section, we are going to collect some information about monolithic groups $L$ containing subgroups $H$ that have these two properties. This will lead to a useful formula for $P_{L,N}^{(p)}(s)$ where $p$ is a certain prime.

Since $N$ is a nonabelian minimal normal subgroup of $L$, there exists a finite nonabelian simple group $S$ such that $N = S_1 \times \cdots \times S_r$ with $S_i \cong S$ for $i = 1, \cdots, r$. Let $\phi$ be the map from $N_L(S_1)$ to $\mathrm{Aut}(S)$ induced by the conjugacy action on $S_1$:

$$\begin{array}{rcl} \phi : N_L(S_1) & \to & \mathrm{Aut}(S) \\ l & \mapsto & \begin{pmatrix} S \to S \\ x \mapsto x^l \end{pmatrix}. \end{array}$$

Let $X = \phi(N_L(S_1))$. Then $X$ is an almost simple group with socle $\mathrm{soc}(X) = S = \mathrm{Inn}(S) = \phi(S_1)$. Since $N = S_1 \times \cdots \times S_r$ is a minimal normal subgroup of $L$, the group $L$ acts transitively on the set $\{S_1, \cdots, S_r\}$. Thus $|L : N_L(S_1)| = |\mathrm{Orb}_L(S_1)| = r$. Let $T = \{t_1, \cdots, t_r\}$ be a right transversal of $N_L(S_1)$ in $L$. We define

$$\begin{array}{rcl} \phi_T : L & \to & X \wr \mathrm{Sym}(r) \\ l & \mapsto & (\phi(t_1 l t_{1\pi}^{-1}), \cdots, \phi(t_r l t_{r\pi}^{-1})) \end{array}$$

where $\pi$ is a permutation in $\mathrm{Sym}(r)$ such that $t_i l t_{i\pi}^{-1} \in N_L(S_1)$ for $i = 1, \cdots, r$. Note that the map $\phi_T$ is injective, so we may identify $L$ with its image in $X \wr \mathrm{Sym}(r)$ such that $N = \mathrm{soc}(L)$ is contained in the base group $X^r$ and $S_i$ is contained in the $i$th component $X_i$, where $X_i \cong X$ for every $i = 1, \cdots, r$.

A subgroup $H$ of $L$ is called *useful* if $H$ supplements $N$ in $L$ and $H$ is an intersection of maximal subgroups of $L$. In particular, any maximal subgroup of $L$ not containing $N$ is useful. Let $M$ be a useful maximal subgroup of $L$ and let $Y = \phi(M \cap N)$. We say that $M$ is of *product type* if $Y \neq 1$ and $\mathrm{Inn}(S) \neq Y$, of *diagonal type* if $\mathrm{Inn}(S) = Y$, and of *complement type* if $Y = 1$. If $M$ is of diagonal type, then $M \cap N$ is a subdirect product of $S_1 \times \cdots \times S_r$, so $M \cap N \cong S^u$ with $0 < u < r$ (see [BBE06, p. 28]).

**Lemma 2.2.1** ([DL07a, Lemma 2.1])**.** *Let $Y$ be a maximal subgroup of $X$ such that $YS = X$. Then $K = (Y \wr Sym(r)) \cap L$ is a maximal useful subgroup of $L$, with $\phi(N_K(S_1)) = Y$ and $K \cap N = (S \cap Y)^r$.*

*Proof.* Let $R = Y \wr \mathrm{Sym}(r)$ then $KN = (R \cap L)N = RN \cap L = L$. Moreover, $K \cap N = (R \cap L) \cap N = R \cap N = (Y \cap S)^r$. Let $H = \phi(N_K(S_1))$. Since $L = KN$ then $HS = X$. On the other hand, for every $y \in Y \cap S$, $y^r \in K \cap N = (Y \cap S)^r$ and so $y \in H = \phi(N_K(S_1))$. From that, we have that $Y \cap S \leq H$. Thus $Y = HS \cap Y = H(Y \cap S) = H$ since $H = \phi(N_K(S_1)) \leq Y$.

It is shown in [BBE06, Proposition 1.1.16] that any maximal subgroup of an almost simple group has a nontrivial intersection with the socle, so $S \cap Y \neq 1$. Moreover $S \cap Y \trianglelefteq Y$ and it follows that $Y = N_X(S \cap Y)$ since $Y$ is maximal in $X$. So $K = N_L((S \cap Y)^r)$.

Let $M$ be a maximal subgroup of $L$ containing $K$. We claim that $\phi(N_M(S_1)) \neq X$. If so, then from the fact that $Y$ is maximal in $X$ and $Y = \phi(N_K(S_1)) \leq \phi(N_M(S_1))$ we obtain that $Y = \phi(N_M(S_1))$. Then for any $\phi(m) \in \phi(M \cap N)$, $m \in M \cap N$ normalizes $S_1$, so $\phi(m) \in \phi(N_M(S_1)) = Y$. Thus $\phi(M \cap N) = Y \cap S$, so $M \cap N \leq (Y \cap S)^r$. Since $(Y \cap S)^r \leq M \cap N$, we obtain that $M \cap N = (Y \cap S)^r = K \cap N$. Thus $M \leq N_L((S \cap Y)^r) = K$ which implies that $K$ is maximal in $L$, and the Lemma is proved.

*Proof of the claim.* Assume by contradiction that $\phi(N_M(S_1)) = X$. Let $x = \phi(m) \in X = \phi(N_M(S_1))$ and $t = \phi(n) \in \phi(M \cap N)$. Then we have that $t^x = \phi(n^m) \in \phi(M \cap N)$ since $M \cap N \triangleleft M$. Hence $\phi(M \cap N)$ is normalized by $X$, and so $\phi(M \cap N) = S$, thus $M$ is of diagonal type. Therefore, there is a partition $J_1, \cdots, J_u$ of $\{1, \cdots, r\}$ such that

$$M \cap N = \triangle_1 \times \cdots \times \triangle_u \neq S^r$$

where $\triangle_i$ is a diagonal subgroup of $S^{J_i}$. We have that

$$(S \cap Y)^r \leq M \cap N = \triangle_1 \times \cdots \times \triangle_u.$$

This implies $S \cap Y = 1$ which is a contradiction. Hence the claim is proved. □

As a consequence of Lemma 2.2.1, we have the following.

**Corollary 2.2.2.** *The index of $K$ in $L$ is $|L : K| = |X : Y|^r$.*

Hence, we have shown that if $X$ contains a useful maximal subgroup $Y$ then $L$ also contains a useful maximal subgroup $K$ with $K \cap N = (S \cap Y)^r$. More generally, we have the following result.

**Lemma 2.2.3** ([DL07a, Lemma 2.2]). *Suppose that $Y \leq X$ satisfies :*

*(1) $X = YS$.*

*(2) $Y$ is an intersection of maximal subgroups of $X$.*

*Then there exists a useful subgroup $U$ of $L$ which can be written as an intersection of maximal subgroups of $L$ of product type and such that $U \cap N = (Y \cap S)^r$.*

*Proof.* Assume that $Y = Y_1 \cap \cdots \cap Y_s$ with $Y_i$ is maximal in $X$, for $i = 1, \cdots, s$. Since $X = YS$ then $X = Y_iS, i = 1, \cdots, s$. By Lemma 2.2.1, we have that $K_i = (Y_i \wr \mathrm{Sym}(r)) \cap L$ is maximal in $X$ and $K_i \cap N = (Y_i \cap S)^r$ for all $i = 1, \cdots, s$. So all the $K_i$'s are of product type.

Let $U = \bigcap_i K_i$ and $R = Y \wr \mathrm{Sym}(r)$. Since $R \cap L = (Y \wr \mathrm{Sym}(r)) \cap L \leq K_i$, for all $i = 1, \cdots, s$, we get that $R \cap L \leq U$. Moreover, since $(R \cap L)N = L$ then $UN = L$. And we also have

$$U \cap N = \cap_i (K_i \cap N) = \cap_i (Y_i \cap S)^r = (\cap_i (Y_i \cap S))^r = (Y \cap S)^r.$$

In particular, we have

$$|L : U| = |NU : U| = |N : N \cap U| = |N : (Y \cap S)^r| = |S : Y \cap S|^r = |YS : Y|^r = |X : Y|^r.$$

□

So now, for every positive integer $n$, put

$$b_n = b_n(L) = \sum_{\substack{|L:U|=n \\ UN=L}} \mu_L(U).$$

**Lemma 2.2.4** ([DL07a, Lemma 2.3]). *Suppose that the integer $m$ has the following properties :*

- *There exists a prime $p$ which divides the order of $S$ but does not divide $m$.*
- *$X$ contains at least one subgroup $Y$ with $|X : Y| = m, YS = X$ and $\mu_X(Y) \neq 0$. Moreover, $\mu_X(Z) = \mu_X(Y)$ for all $Z$ sharing these properties.*

*Then $b_{m^r} \neq 0$.*

*Proof.* Let $\mu = m^r$. Recall that by the proof of Lemma 2.2.1, a useful maximal subgroup of $L$ of diagonal type has index $|S|^u$ for $0 < u < r$. By hypothesis, $|S|^u$ cannot divide $\mu$ and this implies that a useful subgroup $U$ with $|L : U| = \mu$ can be contained only in maximal subgroups of product type.

Suppose that $U$ is a useful subgroup of $L$ with $|L : U| = \mu$. Let $A = \phi(N_U(S_1))$. Since $UN = L$, we have $AS = X$. Let $T = \{t_1, \cdots, t_r\}$ be a right transversal of $N_U(S_1)$ in $U$. As $UN = L$ and $N \leq N_L(S_1)$, then $N_L(S_1) = N_U(S_1)N$, and we can view $T$ as a right transversal of $N_L(S_1)$ in $L$. We use this transversal to define our embedding:

$$\phi_T : L \to X \wr \mathrm{Sym}(r).$$

Let $U \leq M \leq L$ and $B := \phi(N_M(S_1))$. Notice that $t_i \in U \leq M$ for each $1 \leq j \leq r$, so for $m \in M$ we have that $\phi(t_i m t_{i\pi}^{-1}) \in \phi(N_L(S_1) \cap M) = \phi(N_M(S_1)) = B$, this means $M \leq B \wr \mathrm{Sym}(r)$. So $U \leq A \wr \mathrm{Sym}(r)$ (where $A = N_U(S_1)$).

If $M$ is maximal in $L$ then $M = (B \wr \mathrm{Sym}(r)) \cap L$. By Lemma 2.2.1, if $B$ is maximal in $X$ then $K_B = (B \wr \mathrm{Sym}(r)) \cap L$ is a maximal useful subgroup of $L$ containing $U$. Let $\mathfrak{B}$ be the set of maximal subgroups of $X$ containing $A$ and $\mathfrak{M}$ be the set of maximal subgroups of $L$ containing $U$. So the map $B \mapsto K_B$ is a bijection between $\mathfrak{B}$ and $\mathfrak{M}$. Moreover if $B_1, \cdots, B_s \in \mathfrak{B}$ then

$$K_{B_1} \cap \cdots \cap K_{B_s} = L \cap ((B_1 \cap \cdots \cap B_s) \wr \mathrm{Sym}(r)).$$

Let $E = K_{B_1} \cap \cdots \cap K_{B_s}$, notice that $(B_1 \cap \cdots \cap B_s \cap S)^r \leq E$, then

$$B_1 \cap \cdots \cap B_s \cap S \leq \phi(N_E(S_1)) \leq B_1 \cap \cdots \cap B_s.$$

In addition $\phi(N_E(S_1)) \geq \phi(N_U(S_1)) = A$, we have that

$$\phi(N_E(S_1)) \geq (B_1 \cap \cdots \cap B_s \cap S)A = B_1 \cap \cdots \cap B_s \cap SA = B_1 \cap \cdots \cap B_s.$$

So

$$\phi(N_E(S_1)) = B_1 \cap \cdots \cap B_s.$$

This ensures that the map

$$B_1 \cap \cdots \cap B_s \mapsto L \cap ((B_1 \cap \cdots \cap B_s) \wr \mathrm{Sym}(r))$$

is an ordered-preserving bijection between the subgroup lattice of $X$ generated by $\mathfrak{B}$ and that of $L$ generated by $\mathfrak{M}$. In particular, we have

(1) $U = (A \wr \mathrm{Sym}(r)) \cap L$.

(2) $\mu_L(U) = \mu_X(A)$.

Let $R = A \wr \mathrm{Sym}(r)$, we have

$$|L : U| = |LR : R| = |X \wr \mathrm{Sym}(r) : A \wr \mathrm{Sym}(r)| = |X : A|^r$$

so $|L : U| = \mu = m^r$ implies $|X : A| = m$.

Let

$$\mathfrak{L} = \{Z \leq X \text{ such that } |X : Z| = m, ZS = X, \mu_X(Z) \neq 0\}.$$

By hypothesis $\mathfrak{L} \neq \emptyset$, and there is $\gamma$ satisfying $\mu_X(Z) = \gamma$ for all $Z \in \mathfrak{L}$. Let

$$\mathfrak{U} = \{U \leq L \text{ such that } U \text{ is useful in } L \text{ and } \phi(N_U(S_1)) \in \mathfrak{L}\}.$$

So $\mu_L(U) = \gamma$ for each $U \in \mathfrak{U}$. Thus $b_\mu(L) = \sum_{U \in \mathfrak{U}} \mu_L(U) = \gamma|\mathfrak{U}|$. By hypothesis, $\mathfrak{L} \neq \emptyset$ so $\mathfrak{U} \neq \emptyset$. Hence $b_\mu(L) \neq 0$. □

The number $\mu = m^r$ above is called a *useful index* of $L$, and $m$ is called a useful index of $X$. Moreover, we say that a useful index $m$ is a $u$-useful index when $u$ is a prime divisor of $m$.

**Theorem 2.2.5** ([DL07a, Theorem 2.5])**.** *Suppose that $X$ is an almost simple group with socle $S$. Then it admits a $u$-useful index for any prime divisor $u$ of $|S|$.*

As we've seen, when $X$ has a useful subgroup $Y$ of useful index $m$, then by Lemma 2.2.4, the group $L$ also contains a useful subgroup $U$ of index $|L : U| = |X : Y|^r = m^r$. The converse is also true by the following result.

**Lemma 2.2.6** ([DL04b, Lemma 2])**.** *If $n$ is a useful index of $L$ then there is a subgroup $Y$ of $X$ such that $X = YS$ and $n = |X : Y|^r$.*

*Proof.* Since $b_n \neq 0$, there is a subgroup $H$ of $L$ such that $L = HN, |L : H| = n$ and $\mu_L(H) \neq 0$. If $H$ is contained in some maximal subgroup $M$ of diagonal type, then $S \cap Y = 1$ by the proof of Lemma 2.2.1, and $M \cap N = S^u$ where $0 < u < r$, so $|L : M| = |MN : M| = |N : M \cap N| = |S|^{r-u}$. Thus $|S|$ divides $|L : M|$, hence it divides $|L : H|$ (since

$|L : H| = |L : M||M : H|$), which is a contradiction. If follows that $H$ is an intersection of maximal subgroups $M$ of $L$ of product type.

So we have that $H \cap N = (S \cap Y)^r$ by Lemma 2.2.4 for a suitable supplement $Y$ of $S$ in $X$. Such a supplement $Y$ exists and it is exactly the group $A = \phi(N_H(S_1))$ in the proof of Lemma 2.2.5. Therefore

$$n = |L : H| = |N : H \cap N| = |S : S \cap Y|^r = |YS : Y|^r = |X : Y|^r.$$

□

**Lemma 2.2.7.** *Let $u$ be a positive integer such that there is a prime $p$ that divides the order of $S$ and does not divide $u$. Let $\mathfrak{U}$ be the set of all subgroups $Y$ of $X$ such that $|X : Y| = u$ and $YS = X$. If $\mathfrak{U} \neq \emptyset$ and every subgroup of $\mathfrak{U}$ is maximal, then $u^r$ is a useful index of $L$ and $b_{u^r} < 0$.*

*Proof.* If $\mathfrak{U} \neq \emptyset$ and every $Y \in \mathfrak{U}$ is maximal then by Lemma 2.2.1, there is a maximal subgroup $M$ of $L$ such that $|L : M| = u^r$. So $u^r$ is a useful index of $L$. Let $\mathfrak{L}$ be the set of such maximal subgroups $M$. By the proof of Lemma 2.2.4, we have that

$$b_{u^r} = \gamma.|\mathfrak{L}| = |\mathfrak{L}|.\mu_L(M) = |\mathfrak{L}|.\mu_X(Y) = -|\mathfrak{L}| < 0$$

□

Lemma 2.2.1 shows that if $Y$ is a useful subgroup of $X$ then there exists a useful subgroup $U$ of $L$ such that $U \cap N = (Y \cap S)^r$. Moreover, in the proof of Lemma 2.2.5, we get that $U$ is exactly $U = (Y \wr \mathrm{Sym}(r)) \cap L$, and $\mu_L(U) = \mu_X(Y)$ (note that $Y = \phi(N_U(S_1))$). Such a $U$ satisfies the conditions that

- $U \cap N = (U \cap S_1) \times \cdots \times (U \cap S_r)$;
- $U$ is an intersection of maximal subgroups of product type (by Lemma 2.2.3).

Let $\mathcal{U}_Y$ be the set of such subgroups $U$ with respect to $Y$.

**Proposition 2.2.8.** *If $U$ and $V$ are both in $\mathcal{U}_Y$, then $U$ and $V$ are $E$-conjugate where $E = S_2 \times \cdots \times S_r$. Moreover, the cardinality of $\mathcal{U}_Y$ is*

$$|\mathcal{U}_Y| = |E : N_E(U)| = |X : Y|^{r-1}.$$

*Proof.* We first claim that $N_U(S_1)E \leq N_V(S_1)E$. Indeed let $x \in N_U(S_1)E$. Since $UN = VN$, we have $N_U(S_1)N = N_V(S_1)N$. Hence there is an element $s \in S_1$ such that $xs \in N_V(S_1)E$. Moreover, we have that $\phi(x) \in \phi(N_U(S_1)) = Y$ and $\phi(xs) \in \phi(N_V(S_1)) = Y$, and so $\phi(s) \in Y \cap S$. This implies that $s \in \phi^{-1}(Y \cap S) \cap S_1 = S_1 \cap V$. Hence $x \in N_V(S)E$. By the same argument, we get that $N_V(S_1)E \leq N_U(S_1)E$, and so $N_U(S_1)E = N_V(S_1)E$. Therefore $N_U(S_1)E$ and $N_V(S_1)E$ are supplements of $N/E$ in $N_L(S_1)/E$. By [BBE06, Theorem 1.1.35], two groups $U$ and $V$ are $E$-conjugate.

Now let $k = (s_1, \cdots, s_r) \in E$ (hence $s_1 = 1$), $u = (y_1, \cdots, y_r)\alpha \in U$ and $\pi_1 : U \to Y$ the projection from $U$ to the first component $Y$ of $Y \wr \mathrm{Sym}(r)$, then

$$\pi_1([k, u^{-1}]) = y_1 s_{1\alpha} y_1^{-1} \in Y, \text{ hence } s_{1\alpha} \in Y \cap S.$$

Since $L = UN$, for each $i \in \{1, \cdots, r\}$ there exists $(y_1, \cdots, y_r)\alpha \in U$ with $1\alpha = i$, hence

$$N_E(U) = (Y \cap S)^{r-1}$$

and so

$$|E : N_E(U)| = |S : Y \cap S|^{r-1} = |X : Y|^{r-1}.$$

□

As a consequence of Proposition 2.2.8, we have that

$$\sum_{UN=L} \frac{\mu_L(U)}{|L : U|^s} = \sum_{XS=Y} \frac{|X : Y|^{r-1}\mu_X(Y)}{(|X : Y|^r)^s} = \sum_{YS=X} \frac{\mu_X(Y)}{|X : Y|^{rs-r+1}} \tag{2.6}$$

With our $L, N, X, S$ as above, let

$$P_{L,N}(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s} \quad \text{and} \quad P_{X,S}(rs - r + 1) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}$$

If $p$ does not divide $n$ for some prime $p \in \pi(G)$, then by formula (2.6), we get that $b_n = c_n$. As a consequence, we obtain the following.

**Corollary 2.2.9.** *[Ser08] Assume that $L, N, X, S$ are as above and for a prime $p \in \pi(G)$, we have that*

$$\widetilde{P}_{L,i}^{(p)}(s) = P_{L,N}^{(p)}(s) = P_{X,S}^{(p)}(rs - r + 1).$$

## 2.3 Subgroups of prime index in a finite group

As we have seen in Section 2.2, we have an approximation $P_n^{(p)}(s)$ of each factor $P_n(s)$ in the factorization $P_G(s) = \prod_n P_n(s)$ for each prime $p$. In this section, we discuss another approximation $P_{n,p}(s)$ for $P_n(s)$.

As noticed in Section 2.1, $P_n(s)$ depends on the structure of $P_{L,N}(s)$ where $L$ is the monolithic primitive group associated to the chief factor $N = G_n/G_{n+1}$. Hence, we generally focus on $P_{G,N}(s)$ where $N$ is a minimal normal subgroup of a finite group $G$.

Now let $G$ be a finite group and $N$ a minimal normal subgroup of $G$. The series $P_{G,N}(s)$ can be written as

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

We also have that

$$P_{G,N,p}(s) = \sum_r \frac{b_{p^r}}{(p^r)^s}.$$

Therefore, we focus on subgroups of prime power index in $G$. Guralnick gave us a very useful description for subgroups of prime power index in finite simple groups as the following.

**Theorem 2.3.1.** *[Gur83] Let $S$ be a nonabelian simple group with $K < S$ and $|S : K| = p^a$, $p$ prime. Then one of the following holds:*

*(a) $S = Alt(n)$ and $K \cong Alt(n-1)$ with $n = p^a$.*

*(b) $S = PSL_n(q)$ and $K$ is the stabilizer of a line or hyperplane. Then $|S : K| = (q^n - 1)/(q - 1) = p^a$ ($n$ must be prime).*

*(c) $S = PSL_2(11)$ and $K \cong Alt(5)$.*

*(d) $S = M_{23}$ and $K \cong M_{22}$ or $S = M_{11}$ and $K \cong M_{10}$.*

*(e) $S = PSU_4(2) \cong PSp_4(3)$ and $K$ is a parabolic subgroup of index 27.*

**Corollary 2.3.2.** *The group $PSL_2(7)$ is the only simple group with subgroups of two different prime power indices. Moreover, if $p$ is a prime and a finite nonabelian simple group $S$ contains two subgroups $K_1$ and $K_2$ with $|S : K_1| = p^{a_1}$ and $|S : K_2| = p^{a_2}$ then $a_1 = a_2$.*

This gives us a powerful tool in analyzing the subgroups of prime index in finite groups as the following.

**Proposition 2.3.3.** *[DL02, Theorem 13] Suppose that $N$ is a minimal normal subgroup of a finite group $G$. Let $p$ be a prime and define $\mathcal{H}$ to be the set of proper subgroups of $G$ which supplement $N$ and whose index in $G$ is a power of $p$. Then either $\mathcal{H} = \emptyset$ or there exists a positive integer $a$ such that $|G : H| = p^a$ for any $H \in \mathcal{H}$. In the second case, any $H \in \mathcal{H}$ is a maximal subgroup of $G$.*

*Proof.* Assume that $N$ is abelian. If $H \in \mathcal{H}$ then $|G : H| = p^a$ and $G = HN$. Since $N$ is abelian, $H$ is a complement of $N$ in $G$ and so $|G : H| = |N| = p^a$. Also $H$ is maximal in $G$. Therefore, $\mathcal{H} \neq \emptyset$ if and only if $N$ is a $p$-group and has a complement in $G$. In addition, $\mathcal{H}$ coincides with the set of all complements of $N$ in $G$. Therefore, $|G : H| = p^a$ for all $H \in \mathcal{H}$.

Assume now that $N$ is nonabelian. In this case, there exist a positive integer $r$ and a nonabelian simple group $S$ such that $N = S_1 \times \cdots \times S_r$ with $S_i \cong S$ for $i = 1, \cdots, r$. Let $H$ be a supplement of $N$ in $G$ with $|G : H| = p^a$ for some $0 \neq a \in \mathbb{N}$ and $p$ a prime. Then $|N : H \cap N| = |G : H| = p^a$. Since $H$ acts transitively on the set $\{S_1, \cdots, S_r\}$, we get that either $H \cap N$ is isomorphic to a subgroup of $K^r$ where $K < S$, or $H \cap N \cong S^u$ with $u < r$ (see for example the proof of the O'Nan-Scott Theorem in [LPS88]). As $|N : H \cap N| = p^a$ and $N$ is nonabelian, only the first case occurs since otherwise $p^a = |N : H \cap N| = |S|^u$ would be divisible by a prime divisor $p \neq q$ of $|S|$, which is a contradiction. In particular, $H \cap N$ is isomorphic to a subgroup of $K^r$ with $K$ a proper subgroup of $S$. By Corollary 2.3.2, no proper subgroup of $K$ has $p$-power index in $S$, so, as $|N : N \cap H| = p^a$, we must have $H \cap N \cong K^r$. Also by the Corollary 2.3.2, the uniqueness of the index of $K$ implies that $|G : H| = p^a$ for all $H \in \mathcal{H}$. We need to prove that $H$ is a maximal subgroup : assume that $H$ is contained in a maximal subgroup $H < M < G$ with $|G : M|$ a $p$-power. By arguing as above, we have that $M \cap N \cong Y^r$ with $K < Y < S$, which contradicts Corollary 2.3.2, and so $H$ is maximal in $G$. □

Now let $N = S_1 \times \cdots S_r \cong S^r$ be a minimal normal subgroup of $G$ and $\mathcal{H}$ is the set of maximal supplements $H$ of $N$ in $G$ with $|G : H| = p^a$ for a fixed $0 \neq a \in \mathbb{N}$ and $p$ a

prime. If $\mathcal{H} = \emptyset$ then $P_{G,N,p}(s) = 1$. Otherwise, by Proposition 2.3.3, we have that

$$P_{G,N,p}(s) = 1 + \frac{b_{p^a}}{p^{as}}.$$

Moreover, each $H \in \mathcal{H}$ is maximal, then $\mu_G(H) = -1$, and so $b_{p^a} = -|\mathcal{H}|$. Notice that $p^a = |G : H| = |N : H \cap N| = |S^r : K^r| = |S : K|^r$ where $K < S$ is as in the proof of Proposition 2.3.3. Hence $a = r\alpha$, say. Notice also that $b_{p^a}$ and $\alpha$ depend on the simple group $S$. Hence, we can write $P_{G,N,p}(s)$ as

$$P_{G,N,p}(s) = 1 - \frac{c}{p^{\alpha rs}}, \text{ where } c > 0.$$

Now, we go back to the case of profinite groups. Let $G$ be a finitely generated profinite group and $\{G_i\}_{i\in\mathbb{N}}$ a descending chief series with $\bigcap_i G_i = 1$. As in Section 2.1, $P_G(s)$ can be factorized as $P_G(s) = \prod_{i\in\mathbb{N}} P_i(s)$ where each $P_i(s)$ is the finite Dirichlet series associated to the chief factor $N_i = G_i/G_{i+1}$ and

$$P_i(s) = \widetilde{P}_{L_i,j_i}(s) = P_{L_i,N_i}(s) + \cdots$$

with $L_i$ the monolithic primitive group of which the socle is $N_i$. Let $p$ be a prime in $\pi(G)$, we have that

$$P_{i,p}(s) = \widetilde{P}_{L_i,j_i,p}(s) = 1 - \frac{c_i}{(p^{\alpha_i r_i})^s}.$$

Therefore, we have that

$$P_{G,p}(s) = \prod_{i\in\mathbb{N}} \left(1 - \frac{c_i}{(p^{\alpha_i r_i})^s}\right).$$

Hence, we have proved the following.

**Proposition 2.3.4.** *Let $G$ be a finitely generated profinite group and $p$ a prime. Assume that $P_G(s)$ can be factorized as $P_G(s) = \prod_{i\in\mathbb{N}} P_i(s)$. Then for each $i \in \mathbb{N}$, there exist a positive integer $\alpha_i$ (depending only on $S_i$) and a non-negative integer $c_i$ such that*

$$P_{G,p}(s) = \prod_{i\in\mathbb{N}} \left(1 - \frac{c_i}{(p^{\alpha_i r_i})^s}\right).$$

## 2.4 Rational functions and the Skolem-Mahler-Lech theorem

In this section, we present the tools from number theory which help us deduce the finiteness property relating to a rational Dirichlet series. Let $F(s) = \sum_n a_n/n^s$ be a Dirichlet series with integer coefficients. Assume that $F(s)$ is a rational function, i.e., $F(s)$ is the quotient of two finite series, then by Lemma 1.2.5, its $p$-part

$$F_p(s) = \sum_{r=1}^{\infty} \frac{a_{p^r}}{(p^r)^s}$$

is also rational. Or more generally, we consider a rational formal power series $F(s) = \sum_n a_n x^n$. One of the most important tools is the celebrated Skolem-Mahler-Lech theorem, which has the following useful consequence.

**Proposition 2.4.1** ([vdP89, 5.2.1]). *Let $c_1, \cdots, c_r, \alpha_1, \cdots, \alpha_r$ be algebraic numbers with the property that no quotient $\alpha_i/\alpha_j$ is a non-trivial root of unity. Then the exponential polynomial*

$$\phi(h) = c_1\alpha_1^h + \cdots + c_r\alpha_r^h$$

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

This gives us a tool to deduce the finiteness of a rational product as follows

**Theorem 2.4.2** ([DL06c, 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 $I_n = \{i \in I : n_i \text{ divides } n\}$ 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 $\mathbb{Z}[[x]]$, i.e., $F(x)$ is a quotient of two polynomials, then $I = \bigcup_{n\in\mathbb{N}} I_n$ is finite.*

*Proof.* The hypothesis $(i)$ assures us that $F(x)$ is well defined as a formal power series. Now we study $\log(F(x))$. By the formal Taylor expansion

$$\log(1-x) = -\sum_{n=1}^{\infty} \frac{x^n}{n}$$

we have that

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

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

$$w(n) = \sum_{i\in I_n} n_i \gamma_i^{n/n_i}. \tag{2.7}$$

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

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

for complex numbers $\alpha_i, \beta_i, i = 1, \cdots, s, j = 1, \cdots, r$. Hence

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

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

$$w^*(n) = \alpha_1^n + \cdots + \alpha_s^n - \beta_1^n - \cdots - \beta_r^n. \tag{2.8}$$

Comparing (2.7) and (2.8), we obtain, for every $n \in \mathbb{N}$, the following identity:

$$\alpha_1^n + \cdots + \alpha_s^n - \beta_1^n - \cdots - \beta_r^n = \sum_{i \in I_n} n_i \gamma_i^{n/n_i}. \tag{2.9}$$

Replacing in (2.9) $n$ by $nm$, we have

$$\sum_{i=1}^{s} (\alpha_i^n)^m - \sum_{i=1}^{r} (\beta_i^n)^m - \sum_{i \in I_n} n_i (\gamma_i^{n/n_i})^m = \sum_{i \in I_{nm} \setminus I_n} n_i \gamma_i^{nm/n_i}. \tag{2.10}$$

Thus the exponential polynomial

$$\phi_n(m) = \sum_{i=1}^{s} (\alpha_i^n)^m - \sum_{i=1}^{r} (\beta_i^n)^m - \sum_{i \in I_n} n_i (\gamma_i^{n/n_i})^m \tag{2.11}$$

can be written, by (2.10), as

$$\phi_n(m) = \sum_{i \in I_{nm} \setminus I_n} n_i \gamma_i^{nm/n_i}. \tag{2.12}$$

Let

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

To apply Proposition 2.4.1 to the exponential polynomial $\phi_n(m)$ 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 $x, y \in \{\alpha_i, \cdots, \alpha_s, \beta_1, \cdots, \beta_r\}$ and let $e$ be the order of the group generated by $\Omega$. Then a ratio of elements of $\Lambda_e = \{\alpha_1^e, \cdots, \alpha_s^e, \beta_1^e, \cdots, \beta_r^e, \gamma_i^{e/n_i} | i \in I_e\}$ 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 any $i \in I$; this implies that

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

Therefore, by equation (2.12),

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

and so the exponential polynomial $\phi_n(m)$ vanishes for infinitely many integers. Hence $\phi_n(m)$ satisfies the hypothesis of Proposition 2.4.1 and thus

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

Then, by identity (2.10), we obtain

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

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 $(i)$,the set $I$ is finite. □

The consequence of the Skolem-Mahler-Lech theorem in Theorem 2.4.2 gives us a tool to deduce the finiteness of an infinite product. However, as noted before, for a non-prosoluble group $G$, the factorization of $P_G(s)$ does not have a nice form as desired. Hence, we need to look for a way to produce another subproduct which is still rational. The reduction maps in Lemma 1.2.5 are not enough. The following slight modification of Proposition 4.3 in [DL07b] helps.

**Proposition 2.4.3.** *Let $F(s)$ be a product of finite Dirichlet series:*

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

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

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

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

$$F^*(s) = \prod_{i \in I} \left(1 + \frac{b_{i,w^{r_i}}}{(w^{r_i})^s}\right) \tag{2.13}$$

*is also rational.*

*Proof.* In the product

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

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

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

Since $F(s)$ is rational, there is a finite Dirichlet series $A(s) = \sum a_n/n^s$ such that $F(s)A(s)$ is a finite series. Let

$$\xi = \min\left\{x \in \mathbb{Q}_{>0} \;\middle|\; x = \frac{n}{w^{v_q(n)/\alpha}} \text{ and } a_n \neq 0\right\}$$

and

$$N = \{n \in \mathbb{N} : n = \xi w^{v_q(n)/\alpha} \text{ and } a_n \neq 0\}.$$

By definition, $v_q(\xi) = 1$, and for each $n \in \mathbb{N}$ such that $n = \xi w^{m/\alpha}$ with $\alpha$ divides $m \in \mathbb{N}$ we have that $v_q(n) = m$. Hence

$$N = \{\xi w^{m/\alpha} : a_{\xi w^{m/\alpha}} \neq 0, m \in \mathbb{N}, \alpha | m\}.$$

Define a new finite Dirichlet series

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

So

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

The coefficient of $1/(\xi w^{m/\alpha+t})^s$ in $F(s)A(s)$ is

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

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

$$\xi w^{m/\alpha+t} = ln > lw^{v_q(n)/\alpha}.$$

Since $v_q(l) + v_q(n) = m + \alpha t$, $l/w^{v_q(l)/\alpha} < \xi$ which is a contradiction. Hence $n = w^{v_q(n)/\alpha}, l \in N$ and $c_n/n^s$ is a term of $F^*(s)$. So the coefficient of $1/(\xi w^{m/\alpha+t})^s$ in $F(s)A(s)$ is the coefficient of $1/(\xi w^{m/\alpha+t})^s$ in $F^*(s)A^*(s)$, and since $A(s)F(s)$ is finite, $F^*(s)A^*(s)$ is also finite, which implies that $F^*(s)$ is rational. □

## 2.5 Tools from representation theory

As noticed in the previous section, in order to obtain the finiteness of the subseries $\widetilde{P}_G(s)$ by applying the Skolem-Mahler-Lech theorem, we need a good analysis of the behaviour of the set $\mathfrak{R}$ of the composition lengths $r_i$ of the non-Frattini factors $G_i/G_{i+1}$ of a chief series of $G$. In this section, we present results from representation theory that enable us to deal with composition lengths of a finitely generated profinite group $G$ with $\pi(G)$ finite.

**Lemma 2.5.1.** *Let $G$ be a finitely generated profinite group. Then for each positive integer $n$, there are only finitely many non-Frattini factors in a chief series whose order is at most $n$.*

*Proof.* Let $\Omega$ be the set of all non-Frattini chief factors with order at most $n$. Let $G_i/G_{i+1} \in \Omega$. Since $G_i/G_{i+1}$ is non-Frattini, there is a maximal subgroup $M_i$ of $G$ such that $G_{i+1} \leq M_i$ and $G = M_i G_i$. In particular, $|G : M_i|$ divides $|G_i/G_{i+1}|$. Thus $|G : M_i|$ is at most $n$. Note that if $i \neq j$ then $M_i \neq M_j$ : if $i < j$ then $G_j \leq G_{i+1}$, thus $M_i = M_i G_j \neq M_j G_j = G$ implies $M_i \neq M_j$. If $\Omega$ is infinite then there are infinitely many maximal subgroups with index at most $n$. This yields a contradiction since being a finitely generated group, $G$ has only finitely many subgroups of a given index (see [Hal50, Section 2]). □

**Corollary 2.5.2.** *Let $G$ be a finitely generated profinite group with $\pi(G)$ is finite. For a given positive integer $u$, there are only finitely many non-Frattini chief factors in a chief series whose composition length is at most $u$.*

*Proof.* Assume that there are infinitely many non-Frattini chief factors whose composition length is at most $u$. One of the consequences of the classification of finite simple groups

is that, for any finite set $\pi$ of prime numbers, there are only finitely many simple groups $S$ with $\pi(S) \subseteq \pi$. In particular, since $\pi(G)$ is finite, then there are only finitely many non-abelian simple groups that appear as composition factors of the non-Frattini chief factors of $G$. Hence, there exist a simple group $S$ and $r \leq u$ such that there are infinitely many factors isomorphic to $S^r$ in a chief series of $G$. But this contradicts to Lemma 2.5.1. □

We would like to know more about the prime divisors of the composition lengths in $\mathfrak{R}$. Note that, if $G_i/G_{i+1}$ is an abelian chief factor of $G$, then $G_i/G_{i+1} \cong C_{p_i}^{r_i}$ where $p_i$ is a suitable prime; in particular $r_i$ is the degree of an irreducible representation of $G/G_{i+1}$ over the field with $p_i$ elements. This motivates us to employ representation theory in studying the composition lengths. We recall some results from [DL07b, Section 5].

Let $\pi$ be a finite set of prime numbers and let $\mathfrak{H}$ be the set of finite simple groups $S$ such that $\pi(S) \subseteq \pi$. Let $\mathfrak{Q}$ be the set of quasisimple groups $Q$ such that $Q/Z(Q) \in \mathfrak{H}$. Since the universal cover of a finite nonabelian simple group is finite (see [Asc00, 33.10]), for each nonabelian simple group $S$, there are only finitely many quasisimple group $Q$ such that $Q/Z(Q) = S$. As the set $\mathfrak{H}$ is finite, it follows that $\mathfrak{Q}$ is a finite set. For every prime $p$, define $\alpha_p$ to be the largest prime dividing the degree of an absolutely irreducible $\mathbb{F}_pQ$-module for some $Q \in \mathfrak{Q}$. Finally, we set

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

**Proposition 2.5.3** ([DL07b, Lemma 5.1])**.** *Let $n$ be the degree of an irreducible linear representation over a finite field of a $\pi$-group $H$. If $q$ is a prime divisor of $n$ then $q \leq \eta$.*

**Corollary 2.5.4.** *Let $G$ be a finitely generated profinite group. If $\pi(G)$ finite then there is a prime $t$ such that no element of $\mathfrak{R}$ is divisible by $t$.*

*Proof.* Let $X/Y \cong S_1 \times \cdots \times S_r \cong S^r$, where $r \in \mathfrak{R}$, be a non-Frattini chief factor of $G$. Let $u$ be a prime divisor of $r$. If $S$ is abelian then $u \leq \eta$ by Proposition 2.5.3. If $S$ is nonabelian, then the conjugacy action of $G/Y$ on the normal subgroup $X/Y$ induces a transitive permutation representation on the set $\{S_1, \cdots, S_r\}$. Thus $r$, and hence $u$, divides the order of $G/Y$. Therefore $u \in \pi(G)$. Since $\pi(G)$ is finite, the result follows. □

**Corollary 2.5.5.** *Let $G$ be a finitely generated profinite group and assume that $\pi(G)$ is finite. Let $(r_i)$ be the sequence of the composition lengths of the non-Frattini factors in a chief series of $G$.*

*Assume that there exists a positive integer $q$ and a sequence $c_i$ of nonnegative integers such that the formal product*

$$H(s) = \prod_i \left(1 - \frac{c_i}{(q^{r_i})^s}\right)$$

*is rational. Then $c_i = 0$ for all but finitely many indices $i$.*

*Proof.* By Corollary 2.5.4, there is a prime $t$ such that $t$ does not divide any $r_i$. In addition, by Corollary 2.5.2, the set $I_n = \{i : r_i \text{ divides } n\}$ is finite for each positive integer $n$. Hence, if $H(s)$ is rational then, by Theorem 2.4.2, the product $H(s)$ is a finite product. The result follows. □

## 2.6 Steps of the proofs

We present our stragegy and the steps of our proofs. Let $G$ be a finitely generated profinite group of which the probabilistic zeta function $P_G(s)$ is rational. Let $\{G_i\}_{i\in\mathbb{N}}$ be a chief series of $G$ satisfying $G_1 = G$, $\bigcap_{i\in\mathbb{N}} G_i = 1$ and $G_i/G_{i+1}$ is a minimal normal subgroup of $G/G_{i+1}$ for each $i \in \mathbb{N}$. Notice that for each $i$, the chief factor $G_i/G_{i+1}$ gives us the following information:

- $G_i/G_{i+1} \cong S_i^{r_i}$ where $S_i$ is a simple group and $r_i$ the composition length of $G_i/G_{i+1}$.
- As described in Section 2.1 , there exists a monolithic group $L_i$ associated to the chief factor $G_i/G_{i+1}$ with $\mathrm{soc}(L_i) \cong S_i^{r_i}$.
- In particular, when $S_i$ is nonabelian, there is also an associated almost simple group $S_i \leq X_i \leq \mathrm{Aut}(S_i)$ whose socle is isomorphic to $S_i$. That is the image of $N_{L_i}(S_i)$ in $\mathrm{Aut}(S_i)$ under the conjugacy action on $S_i$ (as described in Section 2.2 ).

As described in Section 2.1, to every chief factor $G_i/G_{i+1}$, a finite series

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

is associated and the probabilistic zeta function $P_G(s)$ can be factorized as

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

If $G_i/G_{i+1}$ is Frattini, i.e., $G_i/G_{i+1} \leq \mathrm{Frat}(G/G_{i+1})$, then $G_i/G_{i+1}$ is abelian and $P_i(s) = 1$. If $G_i/G_{i+1}$ is non-Frattini then $P_i(s) \neq 1$ and either $G_i/G_{i+1}$ is nonabelian or it is complemented in $G/G_{i+1}$. In particular, let $J$ be the set of indices $i$ with $G_i/G_{i+1}$ non-Frattini. Then we can write $P_G(s)$ as

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

For any series $C(s) = \sum_{n=1}^{\infty} c_n/n^s$, define $\pi(C(s))$ to be the set of the primes dividing the integers $n$ for which $c_n \neq 0$. Notice that if $C(s) = A(s)/B(s)$ is rational then $\pi(C(s)) \subseteq \pi(A(s)) \bigcup \pi(B(s))$ is finite.

- **Step 1 : Prove that $\pi(G)$ is finite**.

We first have the following useful lemma:

**Lemma 2.6.1** ([DL07b, Lemma 3.1])**.** *Let $G$ be a finitely generated profinite group and let $q$ be a prime with $q \notin \pi(P_G(s))$. Then, for any $i \in J$, the following assertions hold*

1. *If $G_i/G_{i+1}$ is a non-Frattini abelian chief factor, then $|G_i/G_{i+1}|$ is not a $q$-power.*
2. *If $G_i/G_{i+1}$ is nonabelian, then the almost simple group $X_i$ has no maximal subgroup of $q$-power index supplementing $S_i$ in $X_i$.*

*Proof.* First note that $G$ has no proper subgroups of $q$-power index : assume for a contradiction that the set $\Omega$ of proper subgroups of $q$-power index in $G$ is not empty. Choose $q^t$ to be the minimal index of all subgroups in $\Omega$. Note that $|G : H| = q^t$ implies that $H$ is maximal in $G$, and consequently $\mu_G(H) = -1$. Therefore the coefficient $a_{q^t} = \sum_{|G:H|=q^t} \mu_G(H)$ is non-zero, which contradicts the definition of $\pi(P_G(s))$.

If $G_i/G_{i+1}$ is a non-Frattini abelian chief factor then $G_i/G_{i+1}$ has a complement $M/G_{i+1}$ in $G/G_{i+1}$. If the order of $G_i/G_{i+1}$ is a $q$-power, then $M$ is a subgroup of $q$-power index in $G$, which is a contradiction. Hence $|G_i/G_{i+1}|$ is a not a $q$-power. This proves the first assertion.

If $G_i/G_{i+1}$ is a nonabelian chief factor and $X_i$ has a maximal subgroup of $q$-power index supplementing $S_i$ in $X_i$, say $q^t$, then by Lemma 2.2.1 and Corollary 2.2.2, the monolithic group $L_i$ has a maximal subgroup of index $(q^t)^{r_i}$. Since $L_i$ is an epimorphic image of $G$,

as a consequence, $G$ itself has a subgroup of $q$-power index, which is a contradiction. The second assertion follows. □

In the case of prosoluble groups, Lemma 2.6.1 leads immediately to the conclusion that $\pi(G)$ is finite if $P_G(s)$ is rational. This is also true for non-prosoluble groups in our assumption in this thesis but the argument is more complicated. However, we also have from Lemma 2.6.1 that $\Gamma$ contains only finitely many abelian groups, where $\Gamma$ is the set of simple groups that appear as composition factors in non-Frattini chief factors of $G$, that is the set of simple groups $S_i$ for $i \in J$. Hence our main purpose in this step is to prove that $\Gamma$ contains only finitely many nonabelian simple groups. Once $\Gamma$ is finite, $\pi(G)$ will immediately be finite by the following result.

**Corollary 2.6.2.** *The set $\pi(G)$ is finite.*

*Proof.* Let $\pi = \bigcup_{i\in J} \pi(G_i/G_{i+1}) = \bigcup_{S\in\Gamma} \pi(S)$. Since $\Gamma$ is finite, it suffices to prove that $\pi(G) = \pi$. Assume, by contradiction, $q \in \pi(G) \setminus \pi$. There exists $i \in \mathbb{N}$ such that $G_i/G_{i+1}$ is a Frattini chief factor of $q$-power order while $q$ does not divide $|G/G_i|$, which is the index of $G_i/G_{i+1}$ in $G/G_{i+1}$. By the Schur-Zassenhaus Theorem, $G_i/G_{i+1}$ has a complement in $G/G_{i+1}$, but this contradicts the assumption that $G_i/G_{i+1}$ is contained in the Frattini subgroup of $G/G_{i+1}$. □

In order to prove that $\Gamma$ is finite, our stragegy is as the following. Let $I$ be the set of indices $i \in J$ such that $S_i$ is nonabelian, and let $\Gamma^*$ be the set of simple groups $S_i$ with $i \in I$. Let $A(s) = \prod_{i\in I} P_i(s)$ and $B(s) = \prod_{i\notin I} P_i(s)$. Notice that $\pi(B(s)) \subseteq \bigcup_{S\in\Gamma\setminus\Gamma^*} \pi(S)$ is finite. Since $P_G(s) = A(s)B(s)$ and $\pi(P_G(s))$ is finite as $P_G(s)$ is rational, we deduce that $\pi(A(s))$ is finite. So there exists a prime $p \notin \pi(A(s))$. We then proceed by showing that $p \in \pi(A(s))$ to produce a contradiction. This step depends on the structure of the simple groups in $\Gamma^*$, i.e., the structure of the group $G$.

- **Step 2: The main proof**.

We have already obtained that $\pi(G)$ is finite. As a consequence of the classification of finite simple groups, there are only finitely many simple groups that occur as composition factors of $G$. To produce the finiteness of $G/\mathrm{Frat}(G)$, we need to prove that each simple

group that occurs as a composition factor in non-Frattini chief factors, just occurs finitely many times, i.e., the set $I_S := \{i \in J : S_i = S\}$ is finite where $S$ is a simple group and $J$ the set of indices $i$ with $G_i/G_{i+1}$ non-Frattini. We first obtain the result when $S$ is abelian as follows.

**Proposition 2.6.3.** *If $S$ is abelian then $I_S$ is a finite set.*

*Proof.*Assume that $S \cong C_q$ for some prime $q$. Let $\mathfrak{T}_q$ be the set of the non abelian simple groups $T \in \mathfrak{S}$ containing a proper subgroup of $q$-power index. By Proposition 2.3.4, we have that

$$P_{G,q}(s) = \prod_{i \in I_S} \left(1 - \frac{c_i}{q^{r_i s}}\right) \prod_{T \in \mathfrak{T}_q} \left(\prod_{j \in I_T} \left(1 - \frac{d_j}{q^{r_j \alpha_T s}}\right)\right)$$

where $c_i > 0$ for each $i \in I_S$ and $d_j \geq 0$ if $j \in I_T$ and $T \in \mathfrak{T}_q$. The set $\mathfrak{S}$, and consequently $\mathfrak{T}_q$, is finite. In particular the set $\{\alpha_T \mid T \in \mathfrak{T}_q\}$ is finite. So by Corollary 2.5.4, there is a prime number $t$ that does not divide any element in $\{r_i \mid i \in I_S\} \bigcup (\bigcup_{T \in \mathfrak{T}_q} \{r_j \alpha_T \mid j \in I_T\})$. Thus from Corollary 2.5.5, we have that $P_{G,p}(s)$ is a finite product. In particular, $I_S$ is finite. □

Let $\mathcal{T}$ be the set of the almost simple groups $X$ such that there exist infinitely many $i \in J$ with $X_i \cong X$ and let $I = \{i \in J : X_i \in \mathcal{T}\}$. The hypothesis combined with Proposition 2.6.3, implies that $J \setminus I$ is finite. Hence the product

$$\prod_{i \in I} P_i(s) \tag{2.14}$$

is still rational. We have to prove that $J$ is finite; this is equivalent to showing that $I = \emptyset$. At this stage, notice that since $\pi(G)$ is finite, there are only finitely many primes appearing in the product (2.14). We will prove that for each such prime $p$, the set $I_p$ of indices $i \in I$ in which $p$ appears is empty. This will complete our proof. In order to do this, we use the mapping in Lemma 1.2.5 and reduction techniques in Section 2.3, then finally the consequence of the Skolem-Mahler-Lech theorem (Corrolary 2.5.5). The techniques will depend on the structure of finite simple groups in $\Gamma^*$.

**Remark 2.6.4.** *Once the set $J$ is finite, it will follow that the group $G$ has only finitely many non-Frattini factors in a chief series. This will immediate imply that $G/\mathrm{Frat}(G)$ is finite, since*

*(see [DL06c, Theorem 4.3]) if so then there is an open normal subgroup $N$ of $G$ such that every chief factor in $N$ is Frattini, whence $N \leq \mathrm{Frat}(G)$ : in fact, in every finite homomorphic image $\overline{G}$ of $G$, each $\overline{G}$-chief factor of $\overline{N}$ is Frattini and so $\overline{N} \leq \mathrm{Frat}(\overline{G})$. Therefore $G/\mathrm{Frat}(G)$ is a finite group.*