Profinite groups with a rational probabilistic zeta function

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof. mr. C. J. J. M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 14 mei 2013
klokke 13.45 uur

door

Duong Hoang Dung

geboren te Dong Nai, Vietnam in 1985

Samenstelling van de promotiecommissie:

Promotores: prof. dr. Hendrik W. Lenstra
prof. dr. Andrea Lucchini (Università degli Studi di Padova)

Overige leden: prof. dr. Bas Edixhoven
prof. dr. Federico Menegazzo (Università degli Studi di Padova)
dr. Bart de Smit
prof. dr. Peter Stevenhagen
prof. dr. Christopher Voll (Universität Bielefeld)

This work was funded by Algant-Doc Erasmus Action and was carried out at Universiteit Leiden and the Università degli Studi di Padova.

Profinite groups with a rational probabilistic zeta function
Duong Hoang Dung
Universiteit Leiden, 2013
AMS 2010 Subj. class. code : 20E18, 20D06, 20P05, 11M41
Printed by CLEUP, `www.cleup.it`
ISBN: 978-88-908647-9-7

To my wife

Table of Contents

Chapter 1

Introduction

1.1 Historical introduction

In the last two decades, there has been a growing interest in the use of probability in finite groups. Probabilistic methods have proved useful in the solutions of several problems concerning finite groups, mainly involving simple groups and permutation groups. We refer to Dixon [Dix02] and Shalev [Sha98a, Sha01] for more detailed surveys.

Our subject apparently begins with a series of seven papers (see [ET65, ET67a, ET67b, ET68, ET71, ET70, ET72]) of Erdős and Turán in which they studied the properties of random permutations. For example, they showed that most permutations in the symmetric groups $\mathrm{Sym}(n)$ have order about $n^{\frac{1}{2}\log n}$ and have about $\log n$ cycles. Dixon used Erdős-Turán theory to prove in [Dix69] an old conjecture of Netto that two randomly chosen elements of the alternating group $\mathrm{Alt}(n)$ generate $\mathrm{Alt}(n)$ with probability tending to 1 as $n \to \infty$. Dixon then conjectured that for every finite simple group S, the probability $P(S, 2)$ that two random elements generate the group S tends to 1 as $|S| \to \infty$. Using the classification of finite simple groups, the latter conjecture was proved by W. M. Kantor and A. Lubotzky in [KL90a] for the classical and small exceptional groups of Lie type, and by M. Liebeck and A. Shalev in [LS95] for the remaining ones (see [Sha98a] for more details).

Whereas for finite groups we can compute the probability by simply counting the number of elements, this is not so for infinite groups. Let us start with a simple problem (see [Man04]). We will abuse the word ”probability” before having a correct definition. We will need, as it will be explained later, to move from abstract groups to their profinite completions. Let $G = \mathbb{Z}$, the infinite cyclic group. This group can be generated by one element, but as only two elements of its infinitely many elements are such generators, the probability that one element generates $\mathbb{Z}$ seems to be 0. So let $p = P(\mathbb{Z}, 2)$ be the probability that two elements generate $\mathbb{Z}$. Choosing two elements at random, they generate some subgroup $n\mathbb{Z}$. Again, the probability that $n = 0$ seems to be 0, so with probability 1, our pair of integers generates a non-trivial subgroup. They lie in $n\mathbb{Z}$ with probability $1/n^2$. Once they lie in $n\mathbb{Z}$, recalling that $n\mathbb{Z} \cong \mathbb{Z}$, they generate $n\mathbb{Z}$ with the same probability p. Hence

$$1 = p\left(\sum_{n=1}^{\infty} \frac{1}{n^2}\right) = p\zeta(2).$$

where $\zeta(s)$ is the Riemann zeta function. So we have that $p = 1/\zeta(2) = 6/\pi^2$. In the same way, we also get that $P(\mathbb{Z}, k) = 1/\zeta(k)$. Applying this to $k = 1$ gives a proof of the divergence of the series $\sum_n 1/n$.

With the same argument as above, one obtains that

$$\sum_{n=1}^{\infty} \frac{a_n(\mathbb{Z}^d)}{n^k} = \zeta(k)\zeta(k-1)\cdots\zeta(k-d+1)$$

where $a_n(\mathbb{Z}^d)$ is the number of subgroup of index n in $\mathbb{Z}^d$ for each n.

On infinite groups, in order to compute probabilities, we need probability measures. As we have seen, our argument needs a probability measure defined on $\mathbb{Z}$ that is both translation invariant and countably additive. And it is easy to see that such a measure does not exist. But on a compact group, it exists and it is known as the Haar measure. More precisely, we will be considering profinite groups, i.e., inverse limits of finite groups. Let us first introduce profinite groups and Haar measures on them.

A *topological group* is a group G which is also a topological space, such that the maps $g \mapsto g^{-1} : G \to G$ and $(g, h) \mapsto gh : G \times G \to G$ are both continuous. An easy example of a topological group is a finite group endowed with the discrete topology. A *profinite group* is a compact Hausdorff topological group whose open subgroups form a base for the neighborhoods of the identity. For such a group G, a subgroup is open if and only if it is closed and has finite index. Hence the family of all open subgroups of G intersects in $\{1\}$. Moreover, a subset of G is open if and only if it is a union of cosets of open normal subgroups.

A second definition of profinite groups is based on the concept of an *inverse limit*. We recall briefly what it is. A *directed set* is a partially ordered set $(I, \leq)$ with the property that for every $i, j \in I$, there exists $k \in I$ such that $k \geq i$ and $k \geq j$. An *inverse system* of sets (or groups, rings or topological spaces) over I is a family of sets (or groups, etc.) $(G_i)_{i \in I}$ with maps (respectively homomorphisms, continuous maps) $\phi_{ij} : G_i \to G_j$ whenever $i \geq j$, satisfying $\varphi_{ii} = Id_{G_i}$ and $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$ whenever $i \geq j \geq k$, where "$f \circ g$ means do g first, then f". The *inverse limit*

$$\varprojlim G_i = \varprojlim (G_i)_{i \in I}$$

is the subset (or subgroup, etc.) of the Cartesian product $\prod_{i \in I} G_i$ consisting of all (g_i) such that $\varphi_{ij}(g_i) = g_j$ whenever $i \geq j$. Hence, if for each i, we let π_i be the projection from $\varprojlim G_k$ to G_i, then for $i \geq j$, we have that $\varphi_{ij} \circ \pi_i = \pi_j$. The inverse limit is universal in the sense that if Y is an object with projections $\lambda_i : Y \to G_i$ satisfying $\varphi_{ij} \circ \lambda_i = \lambda_j$ then there is a unique morphism $\phi : Y \to \varprojlim G_i$ such that $\pi_i \circ \phi = \lambda_i$ for each $i \in I$.

If each G_i is a finite group endowed with the discrete topology and $\prod_{i \in I} G_i$ is given the product topology, then $\varprojlim G_i$ becomes a topological group, and this topological group is profinite.

If I is a family of normal subgroups of finite index of a given group G which is closed under taking finite intersections, we may order I by reverse inclusion, i.e., $N \geq M$ whenever $N \subseteq M$, and obtain an inverse system $(G/N)_{N \in I}$. The maps $\varphi_{N,M}$ are the natural epimorphisms $G/N \to G/M$ for $N \subseteq M$. We now come to the equivalence of the two definitions of profinite groups.

Proposition 1.1.1. *[DdSMS99, Proposition 1.3] If G is a profinite group then G is (topologically) isomorphic to* $\varprojlim_{N \lhd_o G}(G/N)$ *where* $N \lhd_o G$ *means that N is an open normal subgroup of G. Conversely, the inverse limit of any inverse system of finite groups is a profinite group.*

For a given abstract group G, $\varprojlim(G/N)$, where N ranges over all normal subgroups of G of finite index, is called the *profinite completion* of G, denoted by $\widehat{G}$. If G is *residually finite*, i.e., the intersection of all above N's is trivial, then G is embedded into its profinite completion (see [Wil98], Proposition 1.4.4).

A typical example for a profinite group is $\mathbb{Z}_p$, the group of p-adic integers, where p is a fixed prime. We can express $\mathbb{Z}_p$ as the following.

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \left\{ (x_n)_{n\geq 0} \in \prod_{n\geq 0} \mathbb{Z}/p^n\mathbb{Z} : \text{for all } n,\ x_{n+1} \equiv x_n \mod p^n \right\}.$$

The profinite completion $\widehat{\mathbb{Z}}$ of $\mathbb{Z}$ is

$$\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \left\{ (x_n)_{n\geq 1} \in \prod_{n=1}^{\infty} \mathbb{Z}/n\mathbb{Z} : \text{for all } n|m,\ a_m \equiv a_n \mod n \right\}.$$

It is also true that

$$\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p.$$

Profinite groups are of interest to number theorists since they in fact arise in number theory as Galois groups of (finite or infinite) Galois extensions of fields, with an appropriate topology. Historically, this is the original motivation for the study of profinite groups, and Galois theory remains the main area of applications of results in profinite groups (see [Wil98, Chapter 3]).

On a profinite group G, there exist Haar measures and they are different from each other by a multiplicative constant. Hence, up to a positive multiplicative constant, there exists a unique normalized Haar measure μ such that $\mu(G) = 1$. Thus, we can consider G as a probability space. If H is an open subgroup of G, then $|G : H| < \infty$ and H is closed, hence measurable. Note that $\mu(H) = \mu(gH) = \mu(Hg)$ and since we may write $G = \bigcup Hg$ as a disjoint union of right cosets of H, we have that $1 = \mu(G) = |G : H|\mu(H)$ and so

$$\mu(H) = \frac{1}{|G : H|}.$$

If H is a closed subgroup of infinite index in G, then H is contained in the intersection of a decreasing sequence of open subgroups, say $H_1 > H_2 > \cdots$, and thus

$$\mu(H) \leq \lim_{i\to\infty} \frac{1}{|G : H_i|} = 0.$$

If $X = \bigcup x_{ij}H_j \bigcup K_l y_{kl}$ is the union of a finite collection of cosets of open subgroups, which we call basic open sets, we can find an open normal subgroup N contained in $\bigcap H_j \cap \bigcap K_l$, and then X is equal to the union of finitely many, say n, cosets of N, in which case

$$\mu(X) = n\mu(N) = \frac{n}{|G : N|}.$$

If X is a union of countable family of basic open sets, we can write X as ascending union $X = \bigcup_{i=1}^{\infty} X_i$ where each X_i is a finite union as above and obtain

$$\mu(X) = \lim_{i \to \infty} \mu(X_i)$$

In particular, if the set $\mathcal{N}$ of all open normal subgroups is countable, this determines the measure for every open set of G. Thus also of every closed sets since $\mu(G \setminus X) = 1 - \mu(X)$. In this case, G is said to be *countably based*. This applies for example when G is finitely generated. For a detailed treatment of Haar measure on profinite groups, the reader is referred to [FJ08, Chapter 18].

When talking about generators of a profinite group, we mean generators as a topological group, i.e., X generates G means that G is the smallest closed subgroup of G containing X. The closure of an arbitrary subset X is $\overline{X} = \bigcap XN$, with N ranging over all open normal subgroups of G. If follows that X generates G if and only if each finite factor G/N is generated by XN/N. Thus G is generated by d elements, say, if and only if each finite factor group G/N can be generated by d elements (see [Wil98, Proposition 4.2.1]).

Let G be a profinite group and μ the normalized Haar measure on G or on some direct power G^k. Fix k and write

$$X(G,k) = \{(x_1, \cdots, x_k) \in G^k | \overline{\langle x_1, \cdots, x_k \rangle} = G\}$$

to denote the set of all k-tuples topologically generating the group G. Since a subset T fails to generate G if and only if T is contained in some maximal open subgroup of G, it is clear that

$$G^k \setminus X(G,k) = \bigcup_{M \max G} M^k$$

where $M \max G$ means that M is a maximal proper open subgroup of G. This is an open subset of G^k so $X(G,k)$ is closed, and hence measurable. We may therefore define

$$P(G,k) = \mu(X(G,k))$$

to be the *probability that a random k-tuple generates* G. Thus $0 \leq P(G,k) \leq 1$, and if $P(G,k) > 0$ then $d(G) \leq k$, where $d(G)$ is the minimal number of generators of G.

Definition 1.1.2. *A group G is called positively finitely generated (PFG) if $P(G,k) > 0$ for some choice of $k \in \mathbb{N}$.*

Hence a PFG group is finitely generated. However, for a d-generated group G, it does not always hold that $P(G,d) > 0$. For example, the group $G = \widehat{\mathbb{Z}}$ is a one-generator group and (see [Bos96])

$$P(\widehat{\mathbb{Z}},k) = \begin{cases} 1/\zeta(k) & , k > 1 \\ 0 & , k = 1 \end{cases}$$

and hence $P(\widehat{\mathbb{Z}},1) = 0$. Kantor and Lubotzky proved in [KL90a, Proposition 11] that the free profinite group of rank d is not PFG if $d \geq 2$. It was observed by Fried and Jarden in 1986 (first edition of [FJ08]) that procyclic groups are PFG. This was extended by Kantor and Lubotzky in [KL90a, Proposition 12] to finitely generated abelian profinite groups. In his 1996 paper, Mann proved that finitely generated prosoluble groups are PFG ([Man96, Theorem 10]), and so are the profinite completions of the groups $\mathrm{SL}(k,R)$ where $k \geq 3$ and R the ring of integers in an algebraic number field. He also indicated that a similar result holds for other simple arithmetic groups that have the congruence subgroup property ([Man96, Theorem 15]). Moreover, Borovik, Pyber and Shalev showed in [BPS96] that finitely generated profinite groups not involving all finite groups as quotients of open subgroups are PFG.

One could ask for necessary and sufficient conditions for a profinite group to be PFG. The following concept is a useful tool for characterizing PFG groups:

Definition 1.1.3. *Let G be a group (not necessarily profinite). We say that G has polynomial maximal subgroup growth (PMSG) if there exists a number s, such that for all numbers n, the number $m_n(G)$ of maximal subgroups of G of index n is at most n^s.*

Mann observed in [Man96, Theorem 3] that if G has PMSG then G is PFG. Let us sketch the proof of this fact. If k elements do not generate the group G then they belong to some maximal M of G. The probability for this event is $|G:M|^{-k}$. Hence

$$1 - P(G,k) \leq \sum_{M \max G} |G:M|^{-k} = \sum_{n>1} m_n(G) n^{-k}.$$

If $m_n(G) \leq n^{\alpha}$ then by choosing $k \geq \alpha + 2$ we see that

$$1 - P(G,k) \leq \sum_{n>1} n^{\alpha-k} \leq \sum_{n>1} n^{-2} < 1$$

which implies that $P(G,k) > 0$. The converse holds but it is not trivial.

Theorem 1.1.4 ([MS96, Theorem 4])**.** *A profinite group is positively finitely generated if and only if it has polynomial maximal subgroup growth.*

Proof. Let us sketch the main stages of the proof. Suppose G is PFG and fix k with $P(G, k) > 0$. Our aim is to show that $m_n(G)$ grows at most polynomially with n.

Step 1 Use the Classification of Finite Simple Groups and the O'Nan-Scott theorem to show that there is a constant c such that the number of core-free maximal subgroups of index n in an arbitrary finite group is at most cn^5. Here, a maximal subgroup M is called core-free if its normal core $\mathrm{core}_G(M) := \bigcap_{g \in G} M^g$ is trivial.

Step 2 Since G is PFG, G is finitely generated. Hence G has at most countably many maximal subgroups. We say that two maximal subgroups are equivalent if they have the same normal core. In each equivalence class, choose a representative with minimal index in G. Let $\{M_i\}_{i \in \mathbb{N}}$ be the set of representatives and for each n, let $q_n(G)$ be the number of indices i such that $|G : M_i| = n$.

Apply the Borel-Cantelli Lemma to deduce that $q_n(G)$ grows polynomially.

Borel-Cantelli Lemma. *Let X_i be a series of events in a probability space X with probabilities p_i $(i \geq 1)$.*

(i) if $\sum p_i = \infty$ and X_i are pairwise independent then with probability 1 infinitely many of the events X_i happen.

(ii) if $\sum p_i < \infty$ then with probability 1 only finitely many of the events X_i happen.

We explain how to apply the lemma. Let X be G^k considered as a probability space, and set $X_i = M_i^k$ for each i. It is easy to see that, if the maximal subgroups M, L of G have different cores, then M^k, L^k are independent events in G^k. Therefore the events X_i are pairwise independent. Obviously, the probability that X_i holds is $p_i = |G : M_i|^{-k}$.

We claim that $\sum p_i < \infty$. Suppose otherwise, then by part (i) of the Borel-Cantelli Lemma, with probability 1, infinitely many of the events X_i happen. Hence $x_1, \cdots, x_k$ lie in infinitely many subgroups M_i with probability 1. This certainly implies $P(G, k) = 0$, a contradiction. Therefore $\sum p_i < \infty$.

Now, note that

$$\sum p_i = \sum |G : M_i|^{-k} = \sum q_n(G) n^{-k}$$

It follows that $\sum q_n(G) n^{-k} < \infty$, so $q_n(G) = o(n^k)$.

Step 3 Prove that $m_n(G)$ is bounded in terms of $q_n(G)$.

If M is a maximal subgroup of G of index n then $\mathrm{core}_G(M) = N_i$ for some i such that $|G : M_i| \leq n$. The number of possibilities for i is then $q_2(G) + \cdots + q_n(G)$. Applying Step 1 to G/N_i, we see that for a given N_i, the number of such maximal subgroups M is at most cn^5. On the other hand, by Step 2 we have $q_n(G) = o(n^k)$. The number of possibilities for M is then

$$m_n(G) \leq cn^5(q_2(G) + \cdots + q_n(G)) = o(n^{k+6})$$

□

Theorem 1.1.4 gives us a characterization of PFG groups in terms of maximal subgroup growth. However, a structural characterization of PMSG groups is still missing.

In the very recent paper [JZP11], Jaikin-Zapirain and Pyber give a semi-structural characterization which really describes which groups are PFG. One of those results is the following:

Theorem 1.1.5. *Let G be a finitely generated profinite group. Then G is PFG if and only if there exists a constant c such that for any almost simple group R, any open subgroup H of G has at most $l(R)^{c|G:H|}$ quotients isomorphic to R, where $l(R)$ is the minimal degree of a faithful transitive permutation representation of R.*

The full statement of this result with seven equivalent conditions is stated in [JZP11, Theorem 11.1]. Theorem 1.1.5 immediately implies a positive solution of a well-known open problem of Mann ([Man96]).

Corollary 1.1.6. *[JZP11, Corollary 12.1] Let H be an open subgroup in a PFG group. Then H is also a PFG group.*

In [Man96, Section 5], Mann conjectured that

Conjecture A. *For a PFG group G, the values $P(G,k)$ could be interpolated to an analytic function $P(G,s)$ defined in some right half-plane of the complex plane.*

For example, for $G = \widehat{\mathbb{Z}}$, we have that

$$P(\widehat{\mathbb{Z}},k) = \sum_n \frac{\mu(n)}{n^k} = \frac{1}{\zeta(k)}.$$

Theorem 1.1.7. *[Hal36] If G is a finite group, then the conjecture holds, and*

$$P(G,t) = \sum_{H \leq G} \frac{\mu_G(H)}{|G:H|^t}$$

where μ_G is the Möbius function defined for all subgroups H of G recursively by $\mu_G(G) = 1$ and $\sum_{K \geq H} \mu_G(K) = 0$ if $H < G$.

Proof. Let $\Phi(G,t)$ be the number of ordered t-tuples $(x_1, \cdots, x_t)$ such that $G = \langle x_1, \cdots, x_t \rangle$. Since each t-tuple generates a subgroup of G, we have that

$$\sum_{H \leq G} \Phi(H,t) = |G|^t.$$

Möbius inversion now yields

$$\Phi(G,t) = \sum_{H \leq G} \mu_G(H)|H|^t$$

and hence

$$P(G,t) = \frac{\Phi(G,t)}{|G|^t} = \sum_{H \leq G} \frac{\mu_G(H)}{|G:H|^t}.$$

□

Let G now be a PFG group. As noted already, k elements generate G if and only they do not belong to any maximal subgroup, i.e., they belong to $G \setminus \bigcup_{M \max G} M$. Using the inclusion-exclusion principle, the probability for this is

$$1 - \sum \frac{1}{|G:M|^k} + \sum \frac{1}{|G:M \cap L|^k} - \cdots \tag{S}$$

where $M, L, \cdots$ range over all maximal subgroups of G. This expression makes sense only if each of the infinitely many sums occuring in it converges. We rearrange it as follows. First, choose a descending subgroup base $\{N_i\}$. Then let X_i be the set of maximal subgroups containing N_i. Then $P(G,k)$ is the limit, as $n \to \infty$, of the probability that a random k-tuple does not lie in a maximal subgroup in the set X_n. This probability is a finite sum, consisting of the terms in (S) that involve only maximal subgroups from X_n, and the limit of this sum can be formally rearranged in the form

$$P(G,k) = \sum \frac{\mu(H)}{|G:H|^k} \tag{M}$$

for some coefficients $\mu(H)$, where H ranges over all open subgroups of finite index of G, these being ordered by starting with the subgroups in X_1, and their intersections, arranged in some way, then adding the other intersections of subgroups in X_2, arranged in some way, then adding the remaining ones coming from X_3, etc. Note that the group G itself is included, with coefficient 1. To get a usual Dirichlet series, we have to add together terms corresponding to subgroups of the same index. The probability $P(G,k)$ is actually equal to the sum of the series (M), provided we group together (in parentheses) for each i the subgroups that are added at the ith stage. Thus a candidate for $P(G,s)$ in Conjecture A is the series (M), with the above insertion of parentheses, and with k replaced by a complex variable s. The question is whether this series converges in some half plane. Different choices of the subgroup basis $\{N_i\}$ lead to different groupings of the terms in (M), so we have also to know if two different bases lead to the same function. In particular, it is very interesting to know when the series (M) is convergent as written (without parentheses), or even absolutely convergent.

Since (M) is obtained by rearranging (S), we see that

(i) a subgroup H can occur in (M) with a non-zero coefficient only if H is an intersection of finitely many maximal subgroups. Such a subgroup H is called a *maximal intersection*.

(ii) for such a subgroup, $\mu(H)$ is the difference between the number of ways to express H as the intersection of an even number of maximal subgroups and the way of express it as the intersection of an odd number of maximal subgroups.

Using (ii), it is easily seen that $\mu(H)$ satisfies the defining equalities for the Möbius function μ_G, and hence $\mu(H) = \mu_G(H)$. Here the Möbius function μ_G is defined on the lattice of open subgroups of G by $\sum_{H\leq K\leq G}\mu_G(K) = 0$ unless $H = G$, in which case the sum is 1. This gives us another proof for Theorem 1.1.7. Another similar evaluation of $\mu_G(H)$ is given in [Hal36], namely: $\mu_G(H)$ is the difference between the number of chains of subgroups of even length connecting H to G and the number of such chains of odd length.

Let us give another approach to constructing the function $P(G,s)$ by means of infinite products. Let first G be a finite group and let N be a minimal normal subgroup of G. If $N \leq \mathrm{Frat}(G)$, where $\mathrm{Frat}(G)$ is the Frattini subgroup of G, which is the intersection of all maximal subgroups of G, then $P(G,k) = P(G/N,k)$. In the other case, it is shown in [Gas59, Satz 1] that $P(G,k) = P(G/N,k)P_{G,N}(k)$, where $P_{G,N}(k)$ is given by

$$P_{G,N}(k) = 1 + \sum_{r>0}(-1)^r \sum_{i_1<\cdots<i_r} \frac{\epsilon_{i_1,\cdots,i_r}}{|G : M_{i_1}\cap\cdots\cap M_{i_r}|^k}.$$

Here $M_1,\cdots,M_m$ are the maximal subgroups of G, and $\epsilon_{i_1,\cdots,i_r}$ has the value 1 or 0, according as $HN = G$ or not, where $H = M_{i_1}\cap\cdots\cap M_{i_r}$. Note that $P_{G,N}(k)$ is the probability that a k-tuple generates G, given that it generates G modulo N. By taking a chief series of G and iterating the above formula, we obtain an expression for $P(G,k)$ as a product, indexed by the non-Frattini chief factors in the series. Here a chief series of a finite group G is a series of normal subgroups $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1$ such that each chief factor G_i/G_{i+1}, for $i = 0,\cdots,n-1$, is a minimal normal subgroup of G/G_{i+1}. A chief factor R/S of a finite group G is called non-Frattini if it is not contained in the Frattini subgroup $\mathrm{Frat}(G/S)$.

When G is a profinite group, first of all, we have the following interpretation.

Proposition 1.1.8 ([Man96, Theorem 1]). *Let G be a profinite group. Then we have that $P(G,k) = \inf P(G/N,k)$ where N varies over all open normal subgroups of G. Moreover, if $\{N_i\}$ is a subgroup basis for G consisting of normal subgroups, then $P(G,k) = \inf P(G/N_i,k)$.*

Proof. Since open subgroups of profinite groups are of finite index, the groups G/N are all finite. Hence $P(G/N,k)$, for an open subgroup N, is simply the ratio of the number of k-tuples generating the finite group G/N to the number of all k-tuples. Since the set of all k-tuples generating G, as a subset of G^k, is contained in the union of the cosets of N^k determined by k-tuples generating G/N, we have $P(G,k) \leq P(G/N,k)$. Thus if

$\inf P(G/N,k) = 0$ then certainly $P(G,k) = 0$. If $\inf P(G/N,k) > 0$, then G/N can be generated by k elements for each open normal subgroup N, so is G (see [Wil98, Proposition 4.2.1]). Then G has only finitely many open subgroups of a given index (see [RZ10, Proposition 2.5.1]), and only countably many open subgroups in all. Therefore we can find a descending sequence of basic open normal subgroups $\{M_i\}$. Then if S, S_i denote the sets of k-tuples generating G, and generating $G \bmod M_i$, respectively, we have that $S = \bigcap S_i$ and $S_i \supseteq S_{i+1}$. So $\mu(S) = \inf \mu(S_i) = \lim \mu(S_i)$. Since for each open normal subgroup N we have $P(G/N,k) \geq P(G/M_i,k)$ for some i, we have that $P(G,k) = \inf P(G/N,k)$. Finally, if we take $\{N_i\}$ to be any subgroup basis, then each open normal subgroup N contains some N_i, so that $P(G/N,k) \geq P(G/N_i,k)$ and we have $P(G,k) = \inf P(G/N_i,k)$. □

Let G now be a finitely generated profinite group, let $\{N_i\}$ be a normal descending subgroup base and refine $\{N_i\}$ to a chief series (see Section 2.1 for definition). By Proposition 1.1.8, $P(G,k) = \inf P(G/N_i,k)$. This reduces many of our considerations to the case that G is a finite group. For each factor R/S in this series, express $P(G/S,k)$ as a product as above. In the expression for $P_{G/S,R/S}(k)$ we can, without changing its value, replace the maximal subgroups of G/S by the corresponding maximal subgroups of G.

By Proposition 1.1.8, we can express $P(G,k)$ as an infinite product, indexed by the set of non-Frattini factors in our chief series. Now replace k by the complex variable s to obtain a candidate for $P(G,s)$. We have to know if this product converges, and if products associated to different bases are equal.

The subgroups H that occur inside the factors of the product are maximal intersections, but not all maximal intersections occur. Rather, a maximal intersection H occurs only if it satisfies $HR = G$, where R/S is a factor in the given chief series, and S is the first term in this series that is contained in H. The factor R/S is determined by H, but H may occur more than once in the corresponding factor of the product, because it may be expressed in more than one way as a maximal intersection. For each such expression H occurs with a coefficient 1 or -1, according as the number of maximal subgroups involved is even or odd, so H occurs with coefficient $\mu(H)$. We then can write our product as

$$\prod_{R/S} \left(1 + \sum_{G=HR} \frac{\mu_G(H)}{|G:H|^s} \right). \tag{N}$$

Since the factors in the product are probabilities, they lie between 0 and 1, and writing the product as $\prod(1+x_n)$, its convergence is equivalent of the convergence of the sum $\sum x_n$. We see that the convergence of our product is equivalent to the convergence of a sum that looks like (M), but in which only some of the maximal intersections occur.

Proposition 1.1.9. *[Man96, Proposition 18] Given a descending normal subgroup basis, the series* (M) *and product* (N) *have the same domain of convergence, and in this domain, they define the same function.*

Proof. We compare the partial sum S_i of the series consisting of the intersections of maximal subgroups from X_i and the partial product P_i of the factors corresponding to chief factors above N_i. For an integer k, we have $S_i(k) = P_i(k) = P(G/N_i, k)$. Developing the product P_i, it and S_i are Dirichlet polynomials $\sum u_n/n^s$, which have the same value at all large integers, therefore they have the same coefficients u_n, so $S_i(s) = P_i(s)$ for all s. Since the infinite series and product are the limits of S_i and P_i, the Proposition follows. □

If G is a finite soluble group then, as remarked in [Gas59], the formula for $P_{G,N}(k)$ becomes particularly simple. A subgroup H occurs only if it is a maximal subgroup complementing N, so $P_{G,N}(k) = 1 - k(N)/|N|^k$, where $k(N)$ is the number of complements of N (the exact value of $k(N)$ is given in [Gas59]). Therefore, for a prosoluble group the infinite product associated to a chief series takes the form

$$P(G,k) = \prod(1 - k(N)/|N|^k) \tag{P}$$

where the product runs over all complemented chief factors in this chief series. More generally, for any PFG group the factors corresponding to an abelian N have the same form as in (P), and the proof that for prosoluble groups the above product converges ([Man96, Theorem 19]), shows that for any PFG group, the product of the terms corresponding to abelian chief factors converges.

In a more recent paper (see [Man05]), Mann made the conjecture more precise.

Conjecture B. *Let G be a PFG group. Then the infinite series* (M) *converges absolutely in some right half plane.*

Mann also noted in [Man05] the following.

Theorem 1.1.10. *The series* (M) *converges absolutely in some right half plane if and only if G has polynomially bounded Möbius number (PBMN) (see [Luc11a]), i.e., G has the following two properties:*

(1) $\mu_G(H)$ is bounded by a polynomial function in the index of H;

(2) the number $b_n(G)$ of subgroups H of index n satisfying $\mu_G(H) \neq 0$ grows at most polynomially in n.

Proof. If (M) converges absolutely, then $\mu_G(H)/|G : H|^s \to 0$, so μ grows polynomially. Also, since $\mu_G(H)$ is an integer, the subgroups of index n contribute at least b_n/n^s to the series of absolute values, so b_n also grows polynomially. The converse is equally clear. □

Corollary 1.1.11. *If* (M) *converges absolutely in some half plane, then* (N) *also converges absolutely in some half plane, and the two functions are identical in their common domain of convergence.*

Proof. Assume that (M) converges absolutely, so, by Theorem 1.1.10, b_n and μ are bounded by some power n^t. Note that in the term corresponding to $N = R/S$ in the series (N), we have for each subgroup H occurring there, $R/S \cdot H/S = G/S$ so $|G : H| \leq |R/S| = |N|$. It follows that if we write that term as $1 + x_N$, then $|x_N| \leq |N|^{2t-s}$, and $\sum_{|N| \leq n} |x_N| \leq n^{2t+1-s}$. Thus for s large enough, we have $|x_N| < 1$. Therefore the absolute convergence of (N) is equivalent to that of $\sum x_N$, which holds for $s > 2t + 2$.

Now developing the products (N) and collecting together terms with the same value of $|N|$, we get a Dirichlet series, and a similar collection process applied to (M) yields another Dirichlet series. Both series have the same value $P(G, k)$ for all large integers k, therefore the two series are identical, and define the same function. □

Mann also proved in [Man05] that the conditions in Theorem 1.1.10 are satisfied if G is the completion of $\Gamma(R)$ with respect to the congruence topology, with Γ a simple algebraic group defined over $\mathbb{Z}$ and R the ring of integers in some algebraic number field. In [Luc07] it is proved that the properties (1) and (2) hold if G is a finitely generated prosoluble group. In recent paper [Luc11b], Lucchini proved that the conjecture holds if G has polynomial subgroup growth (PSG) (or more generally, if G contains a normal closed prosoluble subgroup N such that G/N has PSG). Moreover, he also showed in [Luc11b] that the conjecture holds if G is a finitely generated adelic profinite group, i.e., a closed subgroup of the cartesian product $\prod_p \mathrm{SL}(m, \mathbb{Z}_p)$, $m \geq 2$, with $\mathbb{Z}_p$ the ring of the p-adic integers.

In [Luc10], it is proved that in order to decide whether a finitely generated profinite group G has PBMN, it suffices to investigate the behaviour of the Möbius function of the subgroup lattice of the finite monolithic groups, that appear as epimorphic images of G. Here, a finite monolithic group L is a group with a unique minimal normal subgroup. The socle $\mathrm{soc}(G)$ of a finite group G is the subgroup generated by the minimal normal subgroups of G. We say that L is (η_1, η_2)*-bounded* if there exist two constants η_1 and η_2 such that

(1) $b_n^*(L) \leq n^{\eta_1}$, where $b_n^*(L)$ denotes the number of subgroups K of L with $|L : K| = n$ and $L = K \cdot \mathrm{soc}(L)$;

(ii) $|\mu_L(K)| \leq |L : K|^{\eta_2}$ for each $K \leq L$ with $L = K \cdot \mathrm{soc}(L)$.

In [Luc10] the following is proved. Denote by $\Lambda(G)$ the set of finite monolithic groups L such that $\mathrm{soc}(L)$ is nonabelian and L is an epimorphic image of G. A PFG group G has PBMN if and only if there exist η_1 and η_2 such that each $L \in \Lambda(G)$ is (η_1, η_2)-bounded. Let now L be a finite monolithic group with nonabelian socle, then $\mathrm{soc}(L) = S_1 \times \cdots \times S_r$, where the groups S_i are isomorphic simple groups. In the recent paper [Luc11a], Lucchini showed a stronger reduction theorem, which requires us to deal only with almost simple groups: let X_L be the subgroup of $\mathrm{Aut}(S_1)$ induced by the conjugation action of $N_G(S_1)$ on S_1. This X_L is a finite almost simple group, uniquely determined by L (see Chapter 2 for more details). It is proved in [Luc11a] that.

Theorem 1.1.12. *Let L be a monolithic group with nonabelian socle. If the associated almost simple group X_L is (c_1, c_2)-bounded, then L is (η_1, η_2)-bounded with $\eta_1 = 10 + 2(1 + c_1 + c_2)/r$ and $\eta_2 = 2c_2 + 8$.*

Combined with [Luc10, Theorem 1], we have that.

Corollary 1.1.13. *A PFG group has PBMN if there exist c_1 and c_2 such that X_L is (c_1, c_2)-bounded for each L in $\Lambda(G)$.*

This theorem allows us to reformulate the Conjecture B as follows.

Conjecture C. *There exist c_1 and c_2 such that any finite almost simple group is (c_1, c_2)-bounded.*

Recently, Colombo and Lucchini proved in [CL10] that this conjecture is satisfied by the symmetric and alternating groups. This implies

Corollary 1.1.14. *If G is a PFG group and, for each open normal subgroup N of G, all composition factor of G/N are either abelian or alternating groups, then G has PBMN.*

So now, leaving out all analytical concerns, we consider the series (M) as a formal Dirichlet series. Since the group G is finitely generated, it has only finitely many open subgroups of a given index (see [Hal50, Section 2]), for any $n \in \mathbb{N}$ we may define the integer $a_n = \sum_H \mu_G(H)$, where the sum is taken over all open subgroups H of G with $|G : H| = n$. We thus can rewrite the Dirichlet series (M) as

$$P_G(s) := \sum_H \frac{\mu_G(H)}{|G : H|^s} = \sum_{n \in \mathbb{N}} \frac{a_n}{n^s}. \tag{F}$$

The reciprocal of this function is called *the probabilistic zeta function* of G (see [Bos96] and [Man96]). As evidenced by the formula, $P_G(s)$ is tied to the subgroup structure of the group G. Because of this, one can believe that the algebraic combinatorial properties of the series (F) are enough to get back the structural properties of the group G.

As we have seen above, when G is prosoluble, the series (F) becomes the series (P)

$$\prod_N \left(1 - \frac{k(N)}{|N|^s}\right)$$

where $N = R/S$ runs over all non-Frattini chief factors in a chief series of G. Note that when G is prosoluble, being a minimal normal subgroup of a finite soluble group G/S, N is an elementary abelian group and so $|N|$ is a prime power, say q_N. Hence we can rewrite our series as

$$\prod_N \left(1 - \frac{k(N)}{q_N^s}\right).$$

One could ask whether G is a prosoluble group if the associated series of G has the above form. The answer is yes, and in fact we obtain more.

Theorem 1.1.15. *Let G be a finitely generated profinite group. Then the following are equivalent (see [DL04b, Theorem 1] and [Man96])*

(1) The group G is prosoluble.

(2) The series $P_G(s)$ can be written as the product $\prod_i(1 - c_i/q_i^s)$, where $c_i \geq 0$ and q_i is a prime power for each i.

(3) The sequence $\{a_n\}$ is multiplicative, that is, $a_m a_n = a_{mn}$ whenever m and n are coprime.

In particular, Theorem 1.1.15 holds for finite groups. A lot of interesting results have been obtained when G is a finite group. Let us now focus on examples of information one can gain about a finite group G solely from knowing $P_G(s)$. Damian and Lucchini generalized Theorem 1.1.15 to p-soluble groups:

Proposition 1.1.16. *[DL07a] A finite group G is p-soluble if and only if $a_{p^r d} = a_{p^r} a_d$ whenever p and d are coprime.*

One could ask whether we also have a result as in Theorem 1.1.15 for supersolvable groups. In fact, Detomi and Lucchini also described a condition for supersolvable groups.

Proposition 1.1.17. *[DL03b] A finite group G is supersolvable if and only if $P_G(s)$ is a finite product of factors of the form $1 - c_i/p_i^s$ where each p_i is a prime and each c_i is positive.*

This begs the question whether a similar result exists for nilpotent groups, but Gaschütz demonstrated that no such result can exist. Indeed, the functions $P_G(s)$ for $G = C_2 \times C_3 \times C_3$ (nilpotent) and for $G = \mathrm{Sym}(3) \times C_3$ (solvable but not nilpotent) are both equal to

$$\left(1 - \frac{1}{2^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{3}{3^s}\right)$$

Therefore, it is impossible to determine nilpotency strictly from $P_G(s)$. However, Damian and Lucchini did find the following result on nilpotency.

Proposition 1.1.18. *[DL05] A finite group G is nilpotent if and ony if $P_G(H,s)$ divides $P_G(s)$ for all $H \leq G$, where*

$$P_G(H,s) = \sum_{H \leq K \leq G} \frac{\mu_G(K)}{|G:K|^s}.$$

The next piece of data we can get from $P_G(s)$ is the set of primes dividing the order of G.

Proposition 1.1.19. *[DL07a] A prime p divides $|G|$ if and only if p divides n for some n with $a_n \neq 0$.*

We now turn our attention to non-soluble groups, mostly simple groups. The problem of recognizing a simple group from its probabilistic zeta function has been investigated by Lucchini, Damian, Morini in [DL04a, DL06a, DLM04] who proved the following theorem.

Theorem 1.1.20. *Let G be a nonabelian finite simple group, let H be a finite group with trivial Frattini subgroup, and assume that $P_G(s) = P_H(s)$.*

(1) If G is an alternating subgroup or a sporadic simple group, then $G \cong H$.

(2) If G and H are groups of Lie type defined over a field of characteristic p, then $G \cong H$.

Recently Patassini completed this story for the remaining finite simple groups.

Theorem 1.1.21. *[Pat11a, Theorem 1] Let G be a finite simple group and H a finite group. If $P_G(s) = P_H(s)$ then $H/\mathrm{Frat}(H) \cong G$.*

In the very beginning of the history of our subject, Boston conjectured in [Bos96] that $P'_G(1) = 0$ whenever G is a nonabelian simple group. This conjecture was proved and generalized by Shareshian in the following theorem.

Theorem 1.1.22. *[Sha98b] Let G be a finite group. Then $P'_G(1) = 0$ unless $G/O_p(G)$ is cyclic for some prime p.*

As we have known from [Gas59, Satz 1], for any normal subgroup N of a finite group G, the polynomial $P_{G/N}(s)$ divides $P_G(s)$ in the ring of finite Dirichlet series and the quotient $P_G(s)/P_{G/N}(s)$ is nontrivial if N is not in $\mathrm{Frat}(G)$. This implies that $P_G(s)$ is irreducible then $G/\mathrm{Frat}(G)$ is a simple group. We wonder whether the converse holds, in particular whether $P_G(s)$ is irreducible when G is a simple group. The answer is positive for all abelian simple groups since $P_{\mathbb{Z}/p\mathbb{Z}}(s) = 1 - 1/p^s$ for each prime p. Boston showed in [Bos96] that if $G = \mathrm{PSL}(2,7)$ then

$$P_{\mathrm{PSL}(2,7)}(s) = \left(1 - \frac{2}{2^s}\right)\left(1 + \frac{2}{2^s} + \frac{4}{4^s} - \frac{14}{7^s} - \frac{28}{14^s} - \frac{28}{28^s} + \frac{21}{21^s} + \frac{42}{42^s}\right).$$

Hence, the converse is not always true for nonabelian simple groups. However, some results were obtained my Damian, Lucchini and Morini as follows.

Theorem 1.1.23. *[DLM04]*

(1) For any prime $p \geq 5$, the polynomial $P_{Alt(p)}(s)$ is irreducible.

(2) If $p = 2^t - 1$ and $t \equiv 3 \mod 4$ then $P_{PSL(2,p)}(s)$ is reducible.

These were extended by recent results of Patassini appeared in [Pat] and [Pat11b] in the following theorem.

Theorem 1.1.24. *(1) Assume that $k \geq 5$. If $k \leq 4.2 \cdot 10^{16}$ or $k \geq (e^{e^{15}} + 2)^3$, then $P_{Alt(k)}(s)$ is irreducible. If we assume the Riemann Hypothesis, then $P_{Alt(k)}(s)$ is always irreducible.*

(2) Let S be a simple group of Lie type. Then $P_S(s)$ is reducible if and only if $S \cong$ PSL(2,p) for some Mersenne prime p such that $\log_2(p+1) \equiv 3 \bmod 4$.

Brown and Bouc found that letting $s = -1$ gives interesting topological information about the group G. The coset poset $\mathcal{C}(G)$ is the poset of the proper cosets of G ordered by inclusion. We can use a simplicial complex $\Delta(\mathcal{C}(G))$ whose simplices are the finite chains in $\mathcal{C}(G)$ to defined the Euler characteristic $\chi(\mathcal{C}(G))$. We may then define the reduced Euler characteristic $\widetilde{\chi}(\mathcal{C}(G)) = \chi(\mathcal{C}(G)) - 1$. Thanks to an observation of Bouc (see [Bou00]), Brown pointed the following.

Theorem 1.1.25. *[Bro00] Let G be a finite group. Then*

$$P_G(-1) = -\widetilde{\chi}(\mathcal{C}(G)).$$

It is well-known that if $\Delta(\mathcal{C}(G))$ is contractible, then its reduced Euler characteristic $\widetilde{\chi}(\mathcal{C}(G))$ is zero. Hence, if $P_G(-1) \neq 0$, then the simplicial complex associated to the group G is non-contractible. In [Bro00], Brown proved the following.

Proposition 1.1.26. *If G is a finite soluble group, then $P_G(-1) \neq 0$.*

Moreover, Brown conjectured that $P_G(-1) \neq 0$ for every finite group G. Recently, Patassini has given several positive answers to this conjecture:

Theorem 1.1.27. *(1) If G is either $PSL(2,q)$ or a Suzuki group ${}^2B_2(q)$ or a Ree group ${}^2G_2(q)$, then $P_G(-1) \neq 0$ (see [Pat09]).*

(2) If G is a classical group that does not contain non-trivial graph automorphisms, then also $P_G(-1) \neq 0$ (see [Pat11c]).

1.2 Thesis problem

Let G be a finitely generated profinite group and $\{G_n\}$ a chief series of G. Since the factor G/G_n is finite, the Dirichlet series $P_{G/G_n}(s)$ is also finite and belongs to the ring $\mathcal{D}$ of Dirichlet polynomials with integer coefficients. As we have seen above for finite groups, the polynomial $P_{G/G_n}(s)$ is a divisor of $P_{G/G_{n+1}}(s)$ in the ring $\mathcal{D}$, and so there is a Dirichlet polynomial $P_n(s)$ such that $P_{G/G_{n+1}}(s) = P_{G/G_n}(s)P_n(s)$, where $P_n(s) = 1$ if G_n/G_{n+1} is a Frattini factor, i.e., $G_n/G_{n+1} \leq \mathrm{Frat}(G/G_{n+1})$. As we will see in Chapter 2, the Dirichlet series $P_G(s)$ can be written as an infinite formal product $P_G(s) = \prod_{n\in\mathbb{N}} P_n(s)$, and if we change the series $\{G_n\}_{n\in\mathbb{N}}$, the factorization remains the same up to reordering the factors.

It is possible that a Dirichlet polynomial can be written as a formal product of infinitely many non-trivial elements of $\mathcal{D}$, for example, $1 = (1-2^{-s})\prod_{n\in\mathbb{N}}(1+2^{-2^n s})$. So it is not clear whether the formal series $P_G(s) = \prod_{n\in\mathbb{N}} P_n(s)$ is finite only when $P_n(s) = 1$ for all but finitely many $n \in \mathbb{N}$. More generally, we can ask whether one can deduce finiteness properties of G from the fact that $P_G(s)$ is finite. It is not true that if $P_G(s) \in \mathcal{D}$ then G must be finite. Indeed, as noted in [Hal36, Theorem 2.3,], $\mu_G(H) \neq 0$ implies that H is an intersection of maximal subgroups of G. Thus $\mathrm{Frat}(G)$ is contained in H, where $\mathrm{Frat}(G)$ is the Frattini subgroup of G, that is the intersection of the closed maximal subgroups of G. It follows that $P_G(s) = P_{G/\mathrm{Frat}(G)}(s)$. For example (see [LS03, Chapter 11]), let G be a pro-p group with $d(G) = d$, we have $G/\mathrm{Frat}(G) \cong \mathbb{F}_p^d$. We can view $\mathbb{F}_p^d$ as a vector space V of dimension d over the field $\mathbb{F}_p$. The generating k-tuples in V are represented by $d \times k$ matrices of rank d over $\mathbb{F}_p$. Since row rank equals column rank, the number of such matrices is just the number of linearly independent d-tuples in $\mathbb{F}_p^k$, which is

$$(p^k-1)(p^k-p)\cdots(p^k-p^{d-1})$$

(this is zero if $k < d$). Dividing by $|V^{(k)}| = p^{kd}$ we get

$$P(G,k) = \prod_{i=0}^{d-1} \left(1 - \frac{p^i}{p^k}\right)$$

and so

$$P_G(s) = \prod_{0 \leq i < d} \left(1 - \frac{p^i}{p^s}\right).$$

Hence, this only gives us hope to get back some properties of $G/\mathrm{Frat}(G)$ instead of G from the knowledge of the probablistic zeta function $P_G(s)$. Notice that the following are equivalent:

- G has only finitely many maximal subgroups.
- $\mathrm{Frat}(G)$ has finite index.
- Any chief series contains only finitely many non-Frattini factors.

In particular, if $G/\mathrm{Frat}(G)$ is finite then $P_G(s) = P_{G/\mathrm{Frat}(G)}(s)$ is a finite Dirichlet series. We would like to ask about the converse. In particular, it was conjectured in [DL06c] the following.

Conjecture. *Let G be a finitely generated profinite group. Then $P_G(s)$ is rational, i.e., a quotient of two polynomials, only if $G/\mathrm{Frat}(G)$ is a finite group.*

As we have seen above, $P_G(s)$ can be written as an infinite product $P_G(s) = \prod_{n \in J} P_n(s)$ where J is the set of indices n such that $N_n = G_n/G_{n+1}$ is non-Frattini. A tempting argument is that if $P_G(s)$ is a finite series then $P_n(s) = 1$ for all but finitely many $n \in J$ and $G/\mathrm{Frat}(G)$ is finite. However, it is false. The problem becomes difficult and we should be more careful since we can't exclude that a formal product of infinitely many non-trivial finite Dirichlet series is finite. Let us first consider the local version for the case of prosoluble groups. Assume now that G is a finitely generated prosoluble group, and let p be a fixed prime. One could ask what information about G we may obtain if $a_{p^r} = 0$ for almost all $r \in \mathbb{N}$, and whether G contains only finitely many maximal subgroups of p-power index. Notice that the following are equivalent for a prosoluble group G:

- G contains only finitely many maximal subgroups of p-power index.

- A chief series of G contains only finitely many non-Frattini factors of p-power order.

As we have seen above, $P_G(s)$ has an Euler factorization over the set of all prime numbers

$$P_G(s) = \prod_p P_{G,p}(s)$$

where

$$P_{G,p}(s) = \sum_r \frac{a_{p^r}}{p^{rs}} = \prod_{n \in \Omega_p} \left(1 - \frac{c_n}{p^{r_n s}}\right)$$

with Ω_p the set of indices n such that $|G_n/G_{n+1}| = p^{r_n}$ and $c_n \neq 0$. Suppose that the p-factor $P_{G,p}(s)$ is a Dirichlet polynomial, or more generally, that $P_{G,p}(s)$ is a rational function of $1/p^s$. Mann asked in [Man96] whether this implies that G has only finitely many maximal subgroups of p-power index. However, the answer to this question is negative. Detomi and Lucchini proved in [DL06c] the following.

Theorem 1.2.1. *There exists a 2-generated prosoluble group G such that for each prime p*

(1) $P_{G,p}(s)$ is a Dirichlet polynomial.

(2) G contains infinitely many maximal subgroups whose indices are p-powers.

Proof. Let us sketch the construction of this example. First of all, notice that if t_n is the number of irreducible polynomials in $\mathbb{F}_2[x]$ of degree n, then

$$1 - 2x = \prod_n (1 - x^n)^{t_n}.$$

This implies that

$$1 - 2\frac{p}{p^s} = \prod_n \left(1 - \frac{p^n}{p^{ns}}\right)^{t_n}.$$

Let $H = \widehat{\mathbb{Z}}^2$ be the free pro-abelian group of rank 2 and fix an odd prime p. Then

$$P_H(s) = \zeta(s)^{-1}\zeta(s-1)^{-1} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)\left(1 - \frac{p}{p^s}\right).$$

Fix a prime p. For every integer n, the multiplicative group $\mathbb{F}_q^*$ of the finite field $\mathbb{F}_q$ with $q = p^n$ elements acts by right multiplication on the additive group $(\mathbb{F}_q, +)$, which can be viewed as a vector space of dimension n over $\mathbb{F}_p$. Hence the cyclic group C_{p^n-1} has an irreducible representation of degree n over $\mathbb{F}_p$. Since H has at least $p^n - 1$ normal subgroups K_i with $H/K_i \cong C_{p^n-1}$, there are at least $p^n - 1$ irreducible H-modules, say $M_{p,n,i}$, with $1 \leq i \leq p^n - 1$.

Notice that $t_n \leq 2^n \leq p^n - 1$ if p odd and $t_n \leq 2^{2n} - 1$ for each n. For each prime p and each n, we consider the following t_n pairwise non-isomorphic irreducible H-modules:

$$\begin{array}{ll} M_{p,n,1}, \cdots, M_{p,n,t_n}, & \text{for } p \neq 2; \\ M_{2,2n,1}, \cdots, M_{2,2n,t_n}, & \text{for } p = 2. \end{array}$$

Note that $|M_{p,n,i}| = p^n$ for $p \neq 2$ and $|M_{2,2n,i}| = 4^n$, for each $i = 1, \cdots, t_n$. Now consider

$$G := \left(\prod_{\substack{p \text{ prime} \neq 2, \\ n \in \mathbb{N}, \\ i=1,\cdots t_n}} M_{p,n,i} \times \prod_{\substack{n \in \mathbb{N}, \\ i=1,\cdots t_n}} M_{2,2n,i} \right) \rtimes H.$$

Then G is a 2-generated prosoluble group, with infinitely many non-Frattini chief factors of p-power orders: Ω_p is infinite and G contains infinitely many maximal subgroups of p-power indices. However

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

Hence

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

□

This does not answer our first question whether the finiteness of $P_G(s)$ implies that $G/\mathrm{Frat}(G)$ is a finite group. Indeed, the group G constructed has the property that $P_{G,p}(s)$ is finite for each prime p. However, we also have that $P_{G,p}(s) \neq 1$, so $P_G(s) = \prod_p P_{G,p}(s)$ turns out to be infinite. Nevertheless, our conjecture holds for prosoluble groups.

Theorem 1.2.2. *Let G be a finitely generated prosoluble group. Then the following are equivalent:*

(1) $a_n = 0$ for almost all $n \in \mathbb{N}$.

(2) $P_G(s)$ is a finite Dirichlet series in the ring $\mathcal{D}$.

(3) $P_G(s)$ is a rational Dirichlet series in the ring $\mathcal{D}$.

(4) G contains only finitely many maximal subgroups.

Proof. Let us recall briefly the proof of this Theorem. This will give us ingredients to deal with the conjecture in more general cases.

Let first $\pi(G)$ be the set of prime divisors of the indices of the open subgroups of G. The rationality of $P_G(s) = \prod_p P_{G,p}(s)$ implies that $\pi(G)$ is finite and $P_{G,p}(s)$ is a rational function of $1/p^s$ for all $p \in \pi(G)$. Fix a prime $p \in \pi(G)$ and let

$$P_{G,p}(s) = \prod_{n \in \Omega_p} \left(1 - \frac{c_n}{p^{r_n s}}\right).$$

We notice that for each $n \in \Omega_p$, the number r_n is the degree of an irreducible representation of the finite soluble group G/G_{n+1} over the field of p elements. We obtain the information about the composition length r_n by the following useful result from representation theory.

Proposition 1.2.3. *[DL06c] Let n be the degree of an irreducible representation of a finite soluble group X over a finite field. Then if q is a prime divisor of n then $q \leq \max\{\pi(X)\}$, where $\pi(X)$ is the set of prime divisors of X.*

So there is a prime t such that t does not divide any n in Ω_p. The proof now relies on the the following fact, which is a consequence of the Skolem-Mahler-Lech theorem (see [DL06c, Proposition 3.2]).

Theorem 1.2.4. *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. In addition, assume that there exists a prime t such that t does not divide any r_i, $i \in I$ and that for every $n \in \mathbb{N}$, the set $I_n = \{i \in I : r_i \text{ divides } n\}$ is finite. Then I is a finite set.

Applying Theorem 1.2.4, we conclude that Ω_p is finite for each $p \in \pi(G)$. Since $\pi(G)$ is finite, Theorem 1.2.2 is then proved. □

Now, let G be an arbitrary finitely generated profinite group G. We can express $P_G(s)$ as an infinite formal product $P_G(s) = \prod_n P_n(s)$ where $P_n(s)$ is the Dirichlet series associated with the chief factor G_n/G_{n+1}. We would like to prove that if $P_G(s)$ is rational, then $P_n(s) = 1$ for almost all $n \in \mathbb{N}$. This would imply that $G/\mathrm{Frat}(G)$ is finite. In the prosoluble case, we used the Euler factorization $P_G(s) = \prod_p P_{G,p}(s)$. However, $P_G(s)$ admits an Euler factorization over the set of prime numbers if and only if G is prosoluble. Anyway, we can get a kind of Euler factorization over the finite simple groups by collecting together, for any simple group S, all the $P_n(s)$ such that the composition factors of G_n/G_{n+1} are isomorphic to S, as follows:

$$P_G(s) = \prod_S P_G^S(s), \quad \text{where } P_G^S(s) = \prod_{G_n/G_{n+1} \cong S^{r_n}} P_n(s).$$

When we try to work with this generalized Euler factorization, we meet several problems. In the prosoluble case, it is easy to prove that if $P_G(s)$ is rational then $\pi(G)$ is finite and $P_{G,p}(s) = 1$ for all but finitely many primes. In the general case, $\pi(G)$ is finite if and only if $P_G^S(s) = 1$ for almost all simple groups S. Non of these two equivalent facts can be easily deduced from the rationality of $P_G(s)$. Even if we know that $P_G(s) = \prod_S P_G^S(s)$ is the product of finitely many Euler factors $P_G^S(s)$, we cannot easily deduce, as in the prosoluble case, that the rationality of $P_G(s)$ implies the rationality of $P_G^S(s)$ for each S. Even if we know that $P_G^S(s) = \prod_{n \in \Omega_S} P_n(s)$, where $\Omega_S = \{n \in \mathbb{N} : G_n/G_{n+1} \cong S^{r_n}\}$, is rational, we cannot apply the same trick (the consequence of Skolem-Mahler-Lech theorem) used in the prosoluble case, because the series $P_n(s)$ are now more complicated and involve many non-trivial terms. In order to deal with this problem, a clever method is to approximate each $P_n(s)$ by $\widetilde{P_n}(s)$ to produce a new series $\widetilde{P_G}(s) := \prod_n \widetilde{P_n}(s)$ which is still rational. For this, the following crucial remarks seem helpful.

Lemma 1.2.5. *Let $F(s) = \prod_{i \in \mathbb{N}} F_i(s) = \sum_n a_n/n^s$ be an infinite product of finite Dirichlet series $F_i(s)$. Define, for each prime p, the following series*

$$F^{(p)}(s) = \sum_{(n,p)=1} \frac{a_n}{n^s} \quad \text{and} \quad F_p(s) = \sum_r \frac{a_{p^r}}{(p^r)^s}$$

If $F(s)$ is rational then $F^{(p)}(s) = \prod_i F_i^{(p)}(s)$ and $F_p(s) = \prod_i F_{i,p}(s)$ are rational.

Notice that one of these reductions was used in prosoluble case as in Theorem (1.2.2). However, for non-prosoluble cases, these approximations do not ensure that we will get a desired product, i.e., these reductions are still not sufficiently strong to produce subseries $\widetilde{P_n}(s)$ of $P_n(s)$ for each n such that each $\widetilde{P_n}(s)$ is of the form $1 - c_n/(w^{r_n})^s$ as in prosoluble cases, with c_n non-negative and w a fixed positive integer, and such that the product $\prod_n \widetilde{P_n}(s)$ is still rational. Notice also that each Dirichlet series $P_n(s)$ for G_n/G_{n+1} nonabelian depends on the structure of G_n/G_{n+1}. More precisely, since G_n/G_{n+1} is a minimal normal subgroup of the finite group G/G_{n+1}, there is a number r_n and a nonabelian simple group S such that $G_n/G_{n+1} \cong S^{r_n}$. So the series $P_n(s)$ depends strongly on the structure of the simple group S. We will be more precise in Chapter 2. In addition, when $G_n/G_{n+1} \cong S^{r_n}$ is nonabelian, the group G/G_{n+1} permutes r_n simple factors isomorphic to S, and so r_n is the degree of a transitive permutation representation.

By a close investigation of subgroup indices in alternating groups, and some new reduction techniques, Detomi and Lucchini obtained the following result.

Theorem 1.2.6 ([DL07b, Theorem 6.1,p. 464]). *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.*

The following four theorems A-D are the main results of the thesis.

Using the same techniques with a deep analysis of the structure of subgroups of simple groups of Lie type over finite fields with same characteristic, we are able to prove the following.

Theorem A. *Let p be a fixed prime and let G be a finitely generated profinite group such that almost every nonabelian composition factor is a simple group of Lie type over a finite field of characteristic p. If $P_G(s)$ is rational then $G/\mathrm{Frat}(G)$ is a finite group.*

However, the techniques used in the proof are not sufficient to deal with the case of simple groups of Lie type over finite fields of varying characteristic. In Chapter 6, we give an example supporting this. However, with the same ingredients, it is possible to obtain the result for $\mathrm{PSL}(2, p)$ as follows.

Theorem B. *Let G be a finitely generated profinite group such that almost every nonabelian* *composition factor is isomorphic to $PSL(2, p)$ for some odd prime $p \geq 5$. Then $P_G(s)$ is rational only if $G/\mathrm{Frat}(G)$ is finite.*

For the remaining class of finite simple groups, i.e., sporadic simple groups, we obtain the following result.

Theorem C. *If G is a finitely generated profinite group such that almost every nonabelian composition factor is isomorphic to a sporadic simple group and $P_G(s)$ is rational, then $G/\mathrm{Frat}(G)$ is a finite group.*

The techniques used to prove Theorem B and Theorem C can be used to give an affirmative answer for the conjecture in a more general case by mixing up finite simple groups. In particular, the result is as follows.

Theorem D. *Let G be a finitely generated profinite group such that almost every nonabelian composition factor is isomorphic either to $PSL(2, p)$ for some odd prime $p \geq 5$, or to a sporadic simple group, or to an alternating group $Alt(n)$ where either n is an odd prime or n is a power of 2. If $P_G(s)$ is rational then $G/\mathrm{Frat}(G)$ is finite.*

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 μ_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:*

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, "\phi"] & A \rtimes G \arrow[r] \arrow[d, "\Phi"] & G \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & B \arrow[r] & B \rtimes G \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

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 ϕ 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 λ 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

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

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 Ω_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 intersection 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 ϕ be the map from $N_L(S_1)$ to $\mathrm{Aut}(S)$ induced by the conjugacy action on S_1:

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

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 π 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 ϕ_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 ith 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 $M \cap N \lhd M$. 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 $X = Y_i S, i = 1, \cdots, s$. 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 μ 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 γ 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 $N_U(S_1)E \le N_V(S_1)E$. 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 $N_V(S_1)E \le N_U(S_1)E$, 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*

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

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 α 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 α_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 α_i/α_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 Λ_n is a non-trivial root of unity. So define Ω 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 Ω. 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 γ_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 Λ_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 γ_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, α a positive integer and Λ 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

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

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 α 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

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

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

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

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 Ω 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 Ω 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 π 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 nonabelian 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 π 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 α_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 π-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 Ω of proper subgroups of q-power index in G is not empty. Choose q^t to be the minimal index of all subgroups in Ω. 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 Γ contains only finitely many abelian groups, where Γ 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 Γ contains only finitely many nonabelian simple groups. Once Γ 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 Γ 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 Γ 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 Γ^* 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 Γ^*, 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 Γ^*.

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.*

Chapter 3

Simple groups of Lie type

The aim of this chapter is to give a proof for the following theorem.

Theorem A. *Let p be a fixed prime and let G be a finitely generated profinite group such that almost every nonabelian composition factor is a simple group of Lie type over a finite field of characteristic p. If $P_G(s)$ is rational then $G/\mathrm{Frat}(G)$ is a finite group.*

3.1 Simple groups of Lie type

In this section, we will develop machinery to compute explicitly each factor $P_i^{(p)}(s)$ of $P_G^{(p)}(s)$ associated to a nonabelian chief factor $G_i/G_{i+1} \cong S_i^{r_i}$ where S_i is a simple group of Lie type over a field of characteristic p. Moreover, we also give some information about the prime divisors of the denominators in $P_i^{(p)}(s)$. This will help us later in analysing the rationality of the series $P_G(s)$. This section is mostly adapted from Chapter 3 in [Pat11a].

Recall that a *simple group of Lie type S* is the subgroup A^F of fixed points under a Frobenius map F of a connected reductive algebraic group A defined over an algebraically closed field of characteristic $p > 0$.

The simple groups of Lie type can be classified in several ways. For instance, they split into two classes: the Chavelley groups and the Twisted groups (see [Car72]). These groups are completely determined by a simple Lie algebra $\mathcal{L}$ over $\mathbb{C}$, a finite field $\mathbb{K}$ and a symmetry of the Dynkin diagram of $\mathcal{L}$.

In general, for the groups of Lie type, we use the notation of [Car72]. The group is denoted by ${}^kL_l(t^k)$ where $k \in \{1, 2, 3\}$ (if $k = 1$, then k is omitted), L varies over the letters

$A, \cdots, G$, and l is the Lie rank of the Lie algebra, and t^k is a power of a prime number p. In particular, the group ${}^kL_l(t^k)$ is defined over the field $\mathbb{F}_{t^k}$ of characteristic p (so we allow t to be irrational). Finally, we set $q = t$, with the exception given in the Table 3.3. Table 3.3 records the various names we use for the groups of Lie type, which gives us a classification of simple groups of Lie type into classical and exceptional groups.

3.1.1 Basic notions about Lie algebras

Let p be a prime number. Let $\mathbb{K}$ be a field of characteristic p. We denote by S a group of Lie type over the field $\mathbb{K}$. We have that S is either an *untwisted group* or a *twisted group* of Lie type. In both cases, a simple Lie algebra $\mathcal{L}$ over the field $\mathbb{K}$ is associated to S.

If S is an untwisted group of Lie type, then S is a Chevalley group $\mathcal{L}(\mathbb{K})$, which is a certain group of automorphisms of $\mathcal{L}$ over the field $\mathbb{K}$ (see [Car72, Proposition 4.4.3]). If S is a twisted group of Lie type, then S is a subgroup of a Chevalley group $\mathcal{L}(\mathbb{K})$.

Now, let S be our group of Lie type. The following objects are associated to S.

- A Killing form $(-,-)$ on the simple Lie algebra $\mathcal{L}$ over the field $\mathbb{K}$.

- A system of roots Φ in a Cartan subalgebra $\mathcal{C}$ of $\mathcal{L}$ and a system of fundamental roots Π in Φ.

- A Dynkin diagram $\mathcal{D}$, that is a graph with elements in Π as vertices, such that $r \in \Pi$ and $s \in \Pi$ are joined by a bond of strength $\frac{4(r,s)}{(r,r)(s,s)}$ ([Car72]). Table 3.4 shows the classification of simple Lie algebras through their Dynkin diagrams.

- A symmetry ρ of the Dynkin diagram of $\mathcal{L}$. In particular, the order of ρ is 1, 2 or 3. The non-trivial symmetries of the connected Dynkin diagrams are indicated in Table 3.5.

We now give some other notions and remarks on the root systems.

- Given a system of roots Φ and a fundamental system Π in Φ, let Φ^+, Φ^- be the sets of positive and negative roots, respectively, with respect to the fundamental system Φ. We recall that a root $r \in \Phi$ is a linear combination of roots of Π with integer coefficients which are all non-negative if $r \in \Phi^+$ and all non-positive if $r \in \Phi^-$.

- The vector space $\mathcal{C}$ is spanned by Π in $\mathcal{L}$. For $r \in \mathcal{C}$, the linear map $w_r : \mathcal{C} \to \mathcal{C}$ defined by
$$w_r(x) = x - \frac{2(r,x)}{(r,r)}r$$
is called a *reflection*. The Weyl group W of Φ is the subgroup of transformations of $\mathcal{C}$ generated by the reflections $\{w_r : r \in \Phi\}$ (see [Car72, Proposition 2.1.8]). Let $l(w)$ be the length of $w \in W$, defined as the minimal n such that $w = w_{r_1} \cdots w_{r_n}$ for $r_i \in \Pi$, $i \in \{1, \cdots, n\}$. Thus $l(1) = 0$. Moreover, $l(w) = |\Phi^+ \cap w^{-1}(\Phi^-)|$ (see [Car72, Theorem 2.2.2]).

- For a subset K of Π, let $\mathcal{C}_K$ be the subspace of $\mathcal{C}$ spanned by K. Let $\Phi_K = \Phi \cap \mathcal{C}_K$ and let W_K be the subgroup of W generated by the reflections $\{w_r : r \in \Phi_K\}$. Note that Φ_K is a system of roots in $\mathcal{C}_K$, the set K is a fundamental system and the Weyl group of Φ_K is W_K (see [Car72, Proposition 2.5.1]).

- An isometry τ of $\mathcal{C}$ is associated to the symmetry ρ in such a way that $\tau(r)$ is a positive multiple of $\rho(r)$ for each $r \in \Pi$. The isometry τ is uniquely determined by ρ. In particular, we observe that for every $w \in W$, the element $w^\tau = \tau^{-1} w \tau$ belongs to W. Finally, note that ρ and τ are non-trivial if and only if G is twisted.

- Let k be the number of the ρ-orbits of Π. Let $I = \{\mathcal{O}_1, \cdots, \mathcal{O}_k\}$ denote the set of ρ-orbits of Π. For each $J \subseteq I$, let $J^* = \bigcup_{K \in J} K$.

- Let $\mathcal{W}$ denote the subgroup of the Weyl group W consisting of all $w \in W$ such that $w^\tau = w$. For a subset J of I, let $\mathcal{W}_J = W_{J^*} \cap \mathcal{W}$. In particular, if $J = \{\mathcal{O}_i\}$ for some $i \in \{1, \cdots, k\}$, then let $W_i = W_{J^*} = W_{\mathcal{O}_i}$, $\mathcal{W}_i = \mathcal{W}_{J^*} = \mathcal{W}_{\mathcal{O}_i}$ and $\Phi_i = \Phi_{J^*} = \Phi_{\mathcal{O}_i}$.

- Let $\mathcal{D}'$ be the Dynkin diagram of $\mathcal{W}$, that is a graph induced by the Dynkin diagram $\mathcal{D}$ by identifying the nodes in the same ρ-orbit (see [Car72, 13.3.8]). The graph $\mathcal{D}'$ is a graph whose nodes are the elements of I, such that $\mathcal{O}_i \in I$ and $\mathcal{O}_j \in I$ are joined if there exists $r_i \in \mathcal{O}_i$ and $r_j \in \mathcal{O}_j$ such that r_i and r_j are joined in $\mathcal{D}$.

- Let K be a subset of Π. We define D_K to be the set of elements w of W such that $w(r) \in \Phi^+$ for each $r \in K$. For a subset J of I, let $\mathcal{D}_J = D_{J^*} \cap \mathcal{W}$.

- For $J \subseteq I$, let
$$T_{\mathcal{W}_J}(t) = \sum_{w \in \mathcal{W}_J} t^{l(w)}.$$

3.1.2 The parabolic subgroups of a simple group of Lie type

Let S be a simple group of Lie type defined over a field of characteristic p. Denote by B a Borel subgroup of S. A *parabolic subgroup* of S is a subgroup of S containing a Borel subgroup.

The parabolic subgroups are crucial in our study since they are the subgroups of S that contain a Sylow p-subgroup and that are intersection of maximal subgroups. We first state a result about $P_G^{(p)}(s)$ for finite groups.

Lemma 3.1.1 ([DL06a, Lemma 2])**.** *Let P be a Sylow p-subgroup of a finite group G, where p is a prime number. Suppose that each maximal subgroup of G which contains P, also contains $N_G(P)$. Then*
$$P_G^{(p)}(s) = P_G(P, s-1) = P_G(N_G(P), s-1)$$
where, for any subgroup K of G,
$$P_G(K,s) = \sum_{n \in \mathbb{N}} \frac{a_n(G,K)}{n^s} \quad \textit{with} \quad a_n(G,K) = \sum_{\substack{|G:H|=n \\ K \leq H \leq G}} \mu_G(H).$$

Proof. First we claim that $\mu_G(H)|N_H(P)| = \mu_G(H)|N_G(P)|$ for each subgroup $P \leq H \leq G$. Indeed, if $\mu_G(H) = 0$ then we are done. Otherwise, $\mu_G(H) \neq 0$, the subgroup H is an intersection of maximal subgroups of G (see [Hal36, Theorem 2.3]), say $M_1, \cdots, M_t$. Since $P \leq M_i$, by hypothesis we get that $N_G(P) \leq M_i$ for each i. Hence $N_G(P) \leq M_1 \cap \cdots \cap M_t = H$ and so $N_G(P) = N_H(P)$. Now set $\Omega_p = \{H \leq G : v_p(|H|) = v_p(|G|)\}$, where $v_r(n)$ is the r-adic valuation of n. We have that

$$\begin{aligned} P_G^{(p)}(s) &= \sum_{H \in \Omega_p} \frac{\mu_G(H)}{|G:H|^s} = \\ &= \sum_{Q \in \mathrm{Syl}_p(G)} \sum_{Q \leq H} \frac{\mu_G(H)}{|G:H|^s} . \frac{1}{|H:N_H(Q)|} = \\ &= \sum_{Q \in \mathrm{Syl}_p(G)} \sum_{Q \leq H} \frac{\mu_G(H)}{|G:H|^{s-1}} . \frac{1}{|G:N_H(Q)|} = \end{aligned}$$

$$
\begin{aligned}
&= \sum_{P\leq H} \frac{\mu_G(H)}{|G:H|^{s-1}}.\frac{|G:N_G(P)|}{|G:N_H(P)|} = \\
&= \frac{1}{|N_G(P)|}\sum_{P\leq H} \frac{\mu_G(H)|N_H(P)|}{|G:H|^{s-1}} = \\
&= \frac{1}{|N_G(P)|}\sum_{P\leq H} \frac{\mu_G(H)|N_G(P)|}{|G:H|^{s-1}} = \\
&= \sum_{P\leq H} \frac{\mu_G(H)}{|G:H|^{s-1}} = P_G(P,s-1).
\end{aligned}
$$

This proves the first equality of our statement. The second one immediately follows from the previous remark that if $\mu_G(H) \neq 0$ and $P \leq H$ then $N_G(P) \leq H$. □

There is a deep connection between the system of roots and the parabolic subgroups, as shown in the following proposition.

Proposition 3.1.2. *[Car72, Theorem 8.3.4, Section 8.6, Section 14.1] Let S be a simple group of Lie type over $\mathbb{K}$ and let B be a Borel subgroup of S. Let I be the set of ρ-orbits of Π and let $\mathcal{S}_B(S) = \{H \leq S : H \geq B\}$. Then there is a bijection*

$$
\begin{aligned}
\Theta : \mathcal{P}(I) &\rightarrow \mathcal{S}_B(S) \\
J &\mapsto P_J
\end{aligned}
$$

such that

- *$P_J \cap P_K = P_{J\cap K}$ for $J, K \subseteq I$ (so the map is a lattice isomorphism).*
- *$P_\emptyset = B$ and $P_I = S$.*
- *$|P_J| = T_{\mathcal{W}_J}(t)$.*

One may associate to J^* an F-stable parabolic subgroup P_J of S, that is a subgroup of S that contains a Sylow p-subgroup and that is an intersection of maximal subgroups of S. The following result gives us an analysis of $P_G^{(p)}(s)$ through the indices of parabolic subgroups of S.

Theorem 3.1.3 ([DL06a, Theorem 3]). *Let $S = {}^kL_l(t^k)$ be a simple group of Lie type of characteristic p. We have that*

$$P_S^{(p)}(s) = (-1)^{o(I)} \sum_{J\subseteq I} (-1)^{o(J)} |S : P_J|^{1-s} = (-1)^{o(I)} \sum_{J\subseteq I} (-1)^{o(J)} \left(\frac{T_{\mathcal{W}_I}(t)}{T_{\mathcal{W}_J}(t)}\right)^{1-s}$$

where $o(J)$ is the number of ρ-orbits in J.

Proof. Let B be an F-stable Borel subgroup of A. The unipotent radical U of B is a Sylow p-subgroup of S and $N_S(U) = B$. As is well known, a maximal subgroup of S which contains U should contain B, hence it is a maximal parabolic subgroup of S, so we can apply the Lemma 3.1.1 to get that

$$P_S^{(p)}(s) = P_S(B, s-1) = \sum_{B\leq H} \frac{\mu_S(H)}{|S : H|^{s-1}}.$$

The map $J \mapsto P_J$ is an isomorphism between the lattice $\mathcal{P}(I)$ of subsets of I ordered by inclusion, and the lattice of subgroups of S containing B. In particular, $\mu_S(P_J) = \mu_{\mathcal{P}(I)}(J) = (-1)^{o(I)-o(J)}$ (see [Sta97, 3.8.3]). As described in [Car72, Chapter 9] and Proposition 3.1.2, to any subset J of I, a parabolic subgroup W_J of the Weyl group W and a polynomial $T_{\mathcal{W}_J}(t)$ are associated with the property that $T_{\mathcal{W}_J}(t) = |P_J|$. So we have

$$\begin{aligned} P_S^{(p)}(s) &= \sum_{B\leq H} \frac{\mu_S(H)}{|S : H|^{s-1}} = \sum_{J\subseteq I} \frac{\mu_S(P_J)}{|S : P_J|^{s-1}} \\ &= \sum_{J\subseteq I} \frac{(-1)^{o(I)-o(J)}}{|S : P_J|^{s-1}} = (-1)^{o(I)} \sum_{J\subseteq I} (-1)^{o(J)} \left(\frac{T_{W_I}(t)}{T_{W_J}(t)}\right)^{1-s}. \end{aligned}$$

□

As we have seen in Proposition 3.1.3, the expression $T_{\mathcal{W}_J}(t)$ depends on the elements of J. However, there is another way to express $T_{\mathcal{W}_J}(t)$, as we will see below.

Let $\mathcal{D}'$ be the graph induced by the Dynkin diagram $\mathcal{D}$ by identifying the nodes in the same ρ-orbit. Let $I := \{\mathcal{O}_1, \cdots, \mathcal{O}_k\}$ be the set of ρ-orbits of the set of nodes of the Dynkin diagram. Denoted by $F_{\mathcal{D}'}(t)$ the polynomial

$$F_{\mathcal{D}'}(t) = \prod_{i=1}^{l} \frac{1-\epsilon_i t^{m_i+1}}{1-\epsilon_i t} \tag{3.1}$$

where e_i and m_i are determined as in Table 3.1 (see [Car72, Theorem 10.2.5, Theorem 14.3.1]).

$\mathcal{D}$	$m_1, \cdots, m_l$	$\mathcal{D}'$	$\epsilon_1, \cdots, \epsilon_l$
A_l	$1, \cdots, l$	$\mathcal{D}$	$1, \cdots, 1$
B_l, C_l	$1, 3, 5, \cdots, 2l-1$	${}^2A_l$	$1, -1, \cdots, (-1)^{l+1}$
D_l	$1, 3, 5, \cdots, 2l-3, l-1$	${}^2B_2$	$1, -1$
E_6	$1, 4, 5, 7, 8, 11$	${}^2D_l$	$1, 1, \cdots, 1, -1$
E_7	$1, 5, 6, 9, 11, 13, 17$	${}^3D_4$	$1, 1, \omega, \omega^2$
E_8	$1, 7, 11, 13, 17, 19, 23, 29$	${}^2E_6$	$1, -1, 1, 1, -1, 1$
F_4	$1, 5, 7, 11$	${}^2F_4$	$1, 1, -1, -1$
G_2	$1, 5$	${}^2G_2$	$1, -1$

Table 3.1: m_i and ϵ_i

In Table 3.1, we set $\omega = e^{2\pi i/3}$. In particular, note that $\mathcal{D} = \mathcal{D}'$ if and only if S is untwisted. In this case, the ϵ_i's are all 1.

By [Car72, Theorem 10.2.3 and Theorem 14.2.1], we have that

$$T_{\mathcal{W}_I}(t) = F_{\mathcal{D}'}(t).$$

If $J \subseteq I$, then $J^* = \bigcup_{K \in J} K$ is a ρ-stable subset of the set of nodes of the Dynkin diagram. For $K \subseteq \Pi$, let $\mathcal{D}_K$ be the subdiagram of $\mathcal{D}$ corresponding to the set of roots K. Let $\mathcal{D}'_J$ be the subdiagram of $\mathcal{D}'$ corresponding to the set of nodes J. Let $\mathcal{D}'_{J_1}, \cdots, \mathcal{D}'_{J_k}$ be the connected components of $\mathcal{D}'_J$. Clearly we have that $J = \bigcup_{i=1}^{k} J_i$ and the union is disjoint. Since J^* is a subset of Π, we have that $\mathcal{D}_{J^*}$ is a subdiagram of $\mathcal{D}$.

Suppose that $\mathcal{D}'_J$ is connected, then just one of the following holds:

- $\mathcal{D}_{J^*}$ is connected and $\mathcal{D}'_J$ is the Dynkin diagram $\mathcal{D}''$ of a simple group of Lie type which is untwisted if and only if $\mathcal{D}_{J^*}$ and $\mathcal{D}'_J$ are isomorphic graphs. In this case, we define $F_{\mathcal{D}'_J}(t) = F_{\mathcal{D}''}(t)$.

- $\mathcal{D}_{J^*}$ is not connected, it has $|\rho|$ components and each of its connected component is isomorphic to the Dynkin diagram $\mathcal{D}''$ of an untwisted group. In this case, we define $F_{\mathcal{D}'_J}(t) = F_{\mathcal{D}''}(t^{|\rho|})$.

Proposition 3.1.4. *[Car72, Theorem 10.2.3, Theorem 14.2.1] Under the above notations, for a subset J of I, we have*

$$T_{\mathcal{W}_J}(t) = \prod_{i=1}^{k} F_{\mathcal{D}'_{J_i}}(t). \tag{3.2}$$

Example 1 Let $S = A_3(t)$. The Dynkin diagram $\mathcal{D}$ of S is A_3 and $I = \{\{r_1\}, \{r_2\}, \{r_3\}\}$.

- Since $\mathcal{D}' = A_3$, we have

$$F_{\mathcal{D}'}(t) = \frac{1-t^2}{1-t}\frac{1-t^3}{1-t}\frac{1-t^4}{1-t} = (1+t)^2(1+t^2)(1+t+t^2).$$

- There are three subsets of I of cardinality 2, that are $J^2_{12} = \{\{r_1\}, \{r_2\}\}, J^2_{23} = \{\{r_2\}, \{r_3\}\}$ and $J^2_{13} = \{\{r_1\}, \{r_3\}\}$. The Dynkin diagrams $\mathcal{D}'_{J^2_{12}}, \mathcal{D}'_{J^2_{23}}$ of the first two subsets J^2_{12} and J^2_{23} are connected and the diagrams $\mathcal{D}'_{(J^2_{12})^*}, \mathcal{D}'_{(J^2_{23})^*}$ are isomorphic to A_2. Thus

$$F_{\mathcal{D}'_{J^2_{12}}}(t) = F_{\mathcal{D}'_{J^2_{23}}}(t) = F_{A_2}(t) = \frac{1-t^2}{1-t}\frac{1-t^3}{1-t} = (1+t)(1+t+t^2).$$

  The diagram $\mathcal{D}'_{(J^2_{13})^*}$ is disconnected and contains two connected components isomorphic to A_1, hence

$$F_{\mathcal{D}'_{J^2_{13}}}(t) = (F_{A_1}(t))^2 = \left(\frac{1-t^2}{1-t}\right)^2 = (1+t)^2.$$

- There are three subsets J^1 of I of cardinality 1. The diagram $\mathcal{D}'_{(J^1)^*}$ is isomorphic to A_1, and

$$F_{\mathcal{D}'_{(J^1)^*}}(t) = 1+t.$$

By Theorem 3.1.3, we obtain

$$\begin{aligned} P_S^{(p)}(s) &= 1 - 2((1+t)(1+t^2))^{1-s} - ((1+t^2)(1+t+t^2))^{1-s} + \\ &+ 3((1+t)(1+t^2)(1+t+t^2))^{1-s} - ((1+t)^2(1+t^2)(1+t+t^2))^{1-s}. \end{aligned}$$

3.1.3 The parabolic subgroups of an almost simple group of Lie type

Now we consider a more general setting. Let X be an almost simple group with socle S isomorphic to a simple group of Lie type over a field of characteristic $p > 0$. Let P be a Sylow p-subgroup of X. Thus $P \cap S$ is a Sylow p-subgroup of S and $B = N_S(P \cap S)$ is a Borel subgroup in S. Given a subgroup H of X, denote by $\mathcal{S}_H(X)$ the set of subgroups K of X such that $K \geq H$.

Lemma 3.1.5 ([Car72, Theorem 8.3.3]). *Let K be a subgroup of S such that $K \geq B$. Then $N_S(K) = K$.*

Lemma 3.1.6 (See [KL90b]). *Let P and B as above. We have that*

1. *$N_X(B) = N_X(P \cap S)$ and $N_X(B)S = X$;*
2. *If M is a maximal subgroup of X such that $M \geq P$ and $MS = X$ then $M \geq N_X(B)$.*

This result implies that

$$\mathcal{S}_{N_X(B)}(X) = \{H \leq X : H \geq N_X(B), HS = X\}.$$

We can generalize Lemma 3.1.1 as follows.

Lemma 3.1.7. *Let r be a prime number, let G be a finite group and let N be a normal subgroup of G. Let R be a Sylow r-subgroup of G. Suppose that if M is a maximal subgroup of G such that $MN = G$ and $R \leq M$, then M contains also $N_G(R)$. Then*

$$P^{(r)}_{G,N}(s) = \sum_{\substack{R \leq H \leq G \\ HN = G}} \frac{\mu_G(H)}{|G : H|^{s-1}}.$$

Proof. The proof is similar to the proof of Lemma 3.1.1 by considering the set $\Omega_r = \{H \leq G : HN = G \text{ and } v_r(|H|) = v_r(|G|)\}$. □

Since $P \cap S \trianglelefteq P$, then $P \trianglelefteq N_X(P) \leq N_X(P \cap S) = N_X(B)$ by Lemma 3.1.6, hence $N_X(P) \leq N_X(B)$. Therefore, Lemma 3.1.6 and Lemma 3.1.7 give us

$$P^{(p)}_{X,S}(s) = \sum_{\substack{P \leq H \leq X \\ HS = X}} \frac{\mu_X(H)}{|X : H|^{s-1}} = \sum_{H \in \mathcal{S}_{N_X(B)}(X)} \frac{\mu_X(H)}{|X : H|^{s-1}}.$$

Let $\mathcal{S}_B^X(S)$ denote the subset of $\mathcal{S}_B(S) = \{H \leq S : H \geq B\}$ given by

$$\mathcal{S}_B^X(S) = \{H \in \mathcal{S}_B(S) : N_X(H) \geq N_X(B)\}.$$

Proposition 3.1.8 ([Pat11a, Proposition 3.9]). *The map $\eta : \mathcal{S}_{N_X(B)}(S) \to \mathcal{S}_B^X(S)$ given by $\eta(H) = H \cap S$ is well-defined. Moreover, η is an isomorphism of posets. In particular $N_X(\eta(H)) = H$ for each $H \in \mathcal{S}_{N_X(B)}(X)$.*

Proof. We show that η is well-defined. Let $H \in \mathcal{S}_{N_X(B)}(X)$. Since $H \cap S \trianglelefteq H$ then $N_X(B) \leq H \leq N_X(H \cap S)$. Moreover, $B \trianglelefteq N_X(B) \leq H$ and $B \leq S$, so $B \leq H \cap S$. Thus $H \cap S \in \mathcal{S}_B^X(S)$.

Let $H \in \mathcal{S}_B^X(S)$. By definition, $N_X(B) \leq N_X(H)$. Since $N_X(B)S = X$ by Lemma 3.1.6, $N_X(H)S = X$. This implies $N_X(H) \in \mathcal{S}_{N_X(B)}(X)$. Its image is $\eta(N_X(H)) = N_X(H) \cap S = N_S(H) = H$ by Lemma 3.1.5. Thus η is surjective.

For any $H, K \in \mathcal{S}_{N_X(B)}(X)$ such that $H \cap S = K \cap S$, we have $N_X(H \cap S) = N_X(K \cap S)$. In order to prove that η is injective, it suffices to prove that $N_X(H \cap S) = H$. It is clear that $H \leq N_X(H \cap S)$ since $H \cap S \trianglelefteq H$. Moreover, since $HS = X$, applying Lemma 3.1.5 we get

$$|X : N_X(H \cap S)| = |S : N_X(H \cap S) \cap S| = |S : N_S(H \cap S)| = |S : H \cap S| = |X : H|$$

so $N_X(H \cap S) = H$. Hence, the map η is injective.

Clearly that η is an isomorphism of posets. □

A *parabolic subgroup* of X is a subgroup H of X such that H supplements S in X and contains $N_X(B)$ for some Borel subgroup B of S, i.e., H is an element of the set $\mathcal{S}_{N_X(B)} = \{K \leq X : K \geq N_X(B), KS = X\}$.

Note that the map

$$\begin{array}{rcl} \Theta : \mathcal{P}(I) & \to & \mathcal{S}_B(S) \\ J & \mapsto & P_J \end{array}$$

is an isomorphism of lattices. Since $N_X(B)$ acts by conjugation on $\mathcal{S}_B(S)$, the group $N_X(B)$ also acts on $\mathcal{P}(I)$. In particular, the action is the following : if $J \subseteq I$ and $g \in N_X(B)$, then J^g is the unique subset of I such that $P_{J^g} = P_J^g$. Moreover, the group $N_X(B)$ acts on I :

if $\mathcal{O}$ is a ρ-orbit, then $\{\mathcal{O}^g\} = \{\mathcal{O}\}^g$. Note that if S is twisted, then the action of $N_X(B)$ is trivial. Assume that S is untwisted. The action of $N_X(B)$ on I can be thought of as an action of $N_X(B)$ on Π. So, any element $g \in N_X(B)$ induces a symmetry ϕ_g of the Dynkin diagram $\mathcal{D}$ of S. Since $X = SN_X(B)$, if $h \in X$ then $h = sg$ for some $s \in S$ and $g \in N_X(B)$. If ϕ_g is not trivial, then we say that h is a *non-trivial graph automorphism* of order $|\phi_g|$ in X (the definition does not depend on the choice of g, since the action does not depend on the choice of g). Observe that $\mathcal{S}_B^X(S)$ is the set of fixed points of $\mathcal{S}_B(S)$ under the action of $N_X(B)$.

If X does not contain non-trivial graph automorphisms, then ϕ_g is the trivial symmetry for each $g \in N_X(B)$. In this case, we have $\mathcal{S}_B^X(S) = \mathcal{S}_B(S)$. If X contains a non-trivial graph automorphism, then S is untwisted and ρ is trivial.

Let $\mathcal{P}^X(I)$ be the subposet of $\mathcal{P}(I)$ consisting of the subsets of I which are unions of $N_X(B)$-orbits of elements of I. Moreover, if $J \in \mathcal{P}^X(I)$, let $\widetilde{J}$ be the set of $N_X(B)$-orbits of J and denote by $o(J)$ the size of $\widetilde{J}$. We have the following generalization of Theorem 3.1.3.

Theorem 3.1.9 ([Pat11a, Theorem 3.10])**.** *Let X and S as above. Then*

$$P_{X,S}^{(p)}(s) = (-1)^{o(I)} \sum_{J \in \mathcal{P}^X(I)} (-1)^{o(J)} |S : P_J|^{1-s} = (-1)^{o(I)} \sum_{J \in \mathcal{P}^X(I)} (-1)^{o(J)} \left(\frac{T_{W_I}(t)}{T_{W_J}(t)} \right)^{1-s}.$$

In particular, if X does not contain non-trivial graph automorphisms, then $P_{X,S}^{(p)}(s) = P_S^{(p)}(s)$.

Proof. By the above consideration, we obtain an isomorphism of posets $\eta : \mathcal{P}^X(I) \to \mathcal{S}_{N_X(B)}(X)$ given by $\eta(J) = N_X(P_J)$ for $J \in \mathcal{P}^X(I)$. In particular, we get $\mu_{\mathcal{P}^X(I)}(J) = \mu_X(N_X(P_J))$. Note that $\mu_{\mathcal{P}^X(I)}(J) = (-1)^{o(I)-o(J)}$. Indeed, there is an isomophism between the poset $\mathcal{P}^X(I)$ and the poset $\mathcal{P}(\widetilde{I})$ of subsets of $\widetilde{I}$ given by $J \mapsto \widetilde{J}$. Thus $\mu_{\mathcal{P}^X(I)}(J) = \mu_{\mathcal{P}(\widetilde{I})}(\widetilde{J})$, and by [Sta97, 3.8.3], we get $\mu_{\mathcal{P}(\widetilde{I})}(\widetilde{J}) = (-1)^{o(I)-o(J)}$.

Since $N_X(P_J) \cap S = P_J$, we have that $|X : N_X(P_J)| = |S : P_J|$. By Lemma 3.1.7, we obtain

$$\begin{aligned} P_{X,S}^{(p)}(s) &= \sum_{H \in \mathcal{S}_{N_X(B)}(X)} \frac{\mu_X(H)}{|X : H|^{s-1}} = \sum_{J \in \mathcal{P}^X(I)} \frac{\mu_X(N_X(P_J))}{|X : N_X(P_J)|^{s-1}} = \\ &= \sum_{J \in \mathcal{P}^X(I)} (-1)^{o(I)-o(J)} |S : P_J|^{1-s} = (-1)^{o(I)} \sum_{J \in \mathcal{P}^X(I)} (-1)^{o(J)} |S : P_J|^{1-s}. \end{aligned}$$

□

Example 2 Let X be an almost simple group with socle $S \cong A_3(t)$. When X does not contain graph automorphisms, we have $P^{(p)}_{X,S}(s) = P^{(p)}_S(s)$. The series $P^{(p)}_S(s)$ has been described in example 1. Assume now that X contains a graph automorphism. Here the Dynkin diagram $\mathcal{D} = \mathcal{D}'$ is A_3, and $I = \{\{r_1\}, \{r_3\}, \{r_2\}\}$. Since X contains a graph automorphism, the set of $N_X(B)$-orbits of I is $\widetilde{I} = \{\{\{r_1\}, \{r_3\}\}, \{\{r_2\}\}\}$.

- We have

$$F_{\mathcal{D}'}(t) = F_{A_3}(t) = \frac{1-t^2}{1-t}\frac{1-t^3}{1-t}\frac{1-t^4}{1-t} = (1+t)^2(1+t+t^2)(1+t^2).$$

- Let $J_1 = \{\{r_1\}, \{r_3\}\}$. The diagram $\mathcal{D}_{J_1^*}$ has two connected components isomorphic to A_1, thus

$$F_{\mathcal{D}'_{J_1}}(t) = (F_{A_1}(t))^2 = (1+t)^2.$$

- Let $J_2 = \{\{r_2\}\}$. The diagram $\mathcal{D}_{J_2^*}$ is the Dynkin diagram A_1. So

$$F_{\mathcal{D}'_{J_2}}(t) = F_{A_1}(t) = (1+t).$$

By Theorem 3.1.9, we obtain

$$\begin{aligned} P^{(p)}_{X,S}(s) &= 1 - ((1+t^2)(1+t+t^2))^{1-s} \\ &\quad -((1+t)(1+t^2)(1+t+t^2))^{1-s} + ((1+t)^2(1+t^2)(1+t+t^2))^{1-s}. \end{aligned}$$

Now let p be a fixed prime and S a simple group of Lie type defined over a finite field of characteristic p. In our work, we will deal with prime divisors of $|S|$, which contains factors of the form $p^m - 1$ where $m \in \mathbb{N}$. It was proved (see [Zsi92]) that

Proposition 3.1.10. *Let a and n be integers greater than 1. Then there exists a prime divisor r of $a^n - 1$ such that r does not divide $a^j - 1$ for any j, $0 < j < n$, except exactly in the following cases*

- *$n = 2, a = 2^t - 1$, where $t \geq 2$.*

- *$n = 6, a = 2$.*

If such a prime exists, we call it a *primitive prime divisor* (or *Zsigmondy prime*) for $\langle a, n\rangle$. Observe that there may be more than one primitive prime divisor of $a^n - 1$; we denote by $\langle a, n\rangle$ the set of these primes. Notice that a Zsigmondy prime in $\langle a, n\rangle$ divides the cyclotomic polynomial $\Phi_n(a)$ and does not divide any $\Phi_k(a)$ whenever $k < n$.

Let p be a prime, r a prime distinct from p, and m an integer which is not a power of p. We define:

$$\begin{aligned} \zeta_p(r) &= \min\{z \in \mathbb{N} \mid z \geq 1 \text{ and } p^z \equiv 1 \mod r\} \\ \zeta_p(m) &= \max\{\zeta_p(r) \mid r \text{ prime}, r \neq p, r|m\}. \end{aligned}$$

The value of $\zeta_p(S) := \zeta_p(|S|)$ where S is a simple group of Lie type over $\mathbb{F}_q$ with $q = p^e$ is given the following table (Table 5.2.C in [KL90b]):

S	$\zeta_p(S)$	exceptions
$L_n(p^e)$ $PSp(n, p^e)$, n even, $n \geq 4$ $P\Omega^-(n, p^e)$, n even, $n \geq 8$	ne	$\zeta_p(L_2(p)) = 1$ if $p + 1 = 2^t$ $\zeta(L_6(2)) = 5$ $\zeta_2(PSp(6, 2)) = 4$
$U(n, p^e)$, $n \geq 3$	$2ne$, n odd $2(n-1)e$, n even	$\zeta_2(U_4(2)) = 4$
$P\Omega^+(n, p^e)$, n even, $n \geq 8$	$e(n-2)$	$\zeta_2(\Omega^+(8, 2)) = 4$
$\Omega(n, p^e)$, qn odd, $n \geq 7$	$e(n-1)$	
${}^2B_2(p^e)$	$4e$	
$G_2(p^e)(p^e \geq 3)$, ${}^2G_2(3^e)(3^e \geq 27)$	$6e$	
$F_4(p^e)$, ${}^2F_4(2^e)$, $E_6(p^e)$, ${}^3D_4(p^e)$	$12e$	
${}^2E_6(p^e)$	$18e$	
$E_7(p^e)$	$18e$	
$E_8(p^e)$	$30e$	

Table 3.2: Level of Zsigmondy primes

Proposition 3.1.11. *Let L be a monolithic group with socle N and assume that $N = S^r$ with S a simple group of Lie type defined over a field of characteristic p. Let $\tau \in \langle p, \zeta_p(S)\rangle$. Consider the Dirichlet series*

$$P^{(p)}_{L,N}(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}.$$

Then

(a) If $b_n \neq 0$ then τ divides n. More precisely, $v_\tau(n) = r\alpha$ with $\alpha = v_\tau(p^{\zeta_p(S)} - 1)$.

(b) If $m > \zeta_p(S)$ and some primitive prime divisor of $p^m - 1$ divides n, then $b_n = 0$.

(c) If $n > 1$ is the smallest positive integer such that $b_n \neq 0$ then $b_n < 0$.

Proof. Let X be the associated almost simple group with socle $\mathrm{soc}(X) = S$ as described in Section 2.2. By Corollary 2.2.9 and by using notations from Theorem 3.1.9, we have that

$$\begin{aligned} P^{(p)}_{L,N}(s) = P^{(p)}_{X,S}(rs - r + 1) &= (-1)^{o(I)} \sum_{J \subseteq I} (-1)^{o(J)} (|S : P_J|^r)^{1-s} \\ &= (-1)^{o(I)} \sum_{J \in \mathcal{P}^X(I)} (-1)^{o(J)} \left(\left(\frac{T_{W_I}(t)}{T_{W_J}(t)} \right)^r \right)^{1-s}. \end{aligned}$$

Notice that $T_{W_I}(t)/T_{W_J}(t)$ is always divisible by the cyclotomic polynomial $\Phi_{\zeta_p(S)/e_S}(t)$ and not divisible by $\Phi_f(t)$ for any $f > \zeta_p/e_S$. Hence (a) and (b) follow. Notice also that the smallest positive integer n such that $b_n \neq 0$ corresponds to the parabolic subgroups P_J of S with $o(I) - o(J) = 1$. This implies immediately that $b_n < 0$ which proves (c). □

3.2 The main result

In this section, we give a proof for **Theorem A**. In this proof, we consider a finitely generated profinite group G such that $P_G(s)$ is rational and we assume that there is a prime p and an open normal subgroup H of which every composition factor is either cyclic or isomorphic to a simple group of Lie type over a field of characteristic p.

We fix a descending normal series $\{G_i\}$ of G with the properties that $\bigcap G_i = 1$ and G_i/G_{i+1} is a chief factor of G/G_{i+1}. Let J be the set of indices i with G_i/G_{i+1} non-Frattini. Then by Section 2.1, the probabilistic zeta function $P_G(s)$ can be factorized as

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

where for each i, the finite Dirichlet series $P_i(s) = \sum_n b_{i,n}/n^s$ is associated to the chief factor G_i/G_{i+1}. Let Γ be 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 $i \in J$. We have the the following crucial result.

Proposition 3.2.1. *The set Γ is finite.*

Proof. Since $P_G(s)$ is rational, the set $\pi(P_G(s))$ is finite. It follows from Lemma 2.6.1 that Γ contains only finitely many abelian groups. Assume by contradiction that Γ is infinite. By our assumption, the subset Γ^* of the simple groups in Γ that are of Lie type over a field of characteristic p is infinite. In particular, the set $\Omega = \{\zeta_p(S) \mid S \in \Gamma^*\}$ is infinite. Let I be the set of indices $i \in J$ such that the composition factors of G_i/G_{i+1} belong to Γ^*. 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 a finite set. Since $P_G(s) = A(s)B(s)$ and $\pi(P_G(s))$ is finite, we deduce that $\pi(A(s))$ is finite. In particular, there exists a positive integer $m \in \Omega$ such that $m \geq 7$ and $\langle p, m\rangle \cap \pi(A(s)) = \emptyset$. Note that we choose $m \geq 7$ to ensure that the set $\langle p, m\rangle$ is non empty (see Proposition 3.1.10). Let Γ_m be the set of positive integers n such that no prime in $\langle p, u\rangle$ divides n if $u > m$ and set

$$\begin{aligned} r &:= \min\{r_i : S_i \in \Gamma^* \text{ and } \zeta_p(S_i) = m\}, \\ I^* &:= \{i \in I : r_i = r \text{ and } S_i \in \Gamma\}, \\ \beta &:= \min\{n > 1 \mid n \in \Gamma_m \text{ and } b_{i,n} \neq 0 \text{ for some } i \in I^*\}. \end{aligned}$$

By Proposition 3.1.11, if $i \in I$ such that $b_{i,\beta} \neq 0$ then $\zeta_p(S_i) = m, r_i = r$ and $b_{i,\beta} < 0$. Hence the coefficient c_β of $1/\beta^s$ in $A(s)$ is

$$c_\beta = \sum_{\substack{i\in I\\ r=r_i}} b_{i,\beta} = \sum_{i\in I^*} b_{i,\beta} < 0.$$

On the other hand, again by Proposition 3.1.11 , all primes in $\langle p, m\rangle$ divide m. But then $\langle p, m\rangle \subseteq \pi(A(s))$, which is a contradiction. Therefore Γ is finite. By Corollary 2.6.2, it follows that $\pi(G)$ is also finite. □

Proof of Theorem A. Let $\mathcal{T}$ be the set of almost simple groups X such that there exist infinitely many $i \in J$ with $X_i \cong X$ and let I be the set of the indices i in J such that $X_i \in \mathcal{T}$. Our assumptions combined with Proposition 2.6.3, imply that $J \setminus I$ is finite. We have to prove that J is finite; this is equivalent to showing that $I = \emptyset$. But then, in order to complete our proof, it suffices to prove the following claim.

Claim. *For every $n \in \mathbb{N}$, the set $I_n = \{i \in I : \zeta_p(S_i) = n\}$ is empty.*

Proof of the claim. Assume that the claim is false and let m be the smallest integer such that $I_m \neq \emptyset$. Since $J \setminus I$ is finite and $P_G(s)$ is rational, the product $\prod_{i \in I} P_i(s)$ is also rational. In particular, the following series is rational:

$$Q(s) = \prod_{i \in I} P_i^{(p)}(s).$$

We distinguish three different cases:

(1) $m = 1, p = 2^t - 1, t \geq 2;$

(2) $m \leq 5, p = 2;$

(3) All the other possibilities.

In case (1) or (3), it follows by Theorem 3.1.10 that $\langle p, t \rangle \neq \emptyset$ for every $t > m + 1$; we set $\sigma = \bigcup_{t > m+1} \langle p, t \rangle \cup \{p\}$. In case (2), we have $\langle 2, t \rangle \neq \emptyset$ whenever $t > 6$ and we set $\sigma = \bigcup_{t>6} \langle 2, t \rangle \cup \{2\}$. Consider $H(s) = Q^{(\sigma)}(s)$, obtained by applying consecutively the homomorphism $P(s) \mapsto P^{(q)}(s)$ for all the primes $q \in \sigma$. The Dirichlet series $H(s)$ is rational. By Proposition 3.1.11, if $i \in I_t$ and $\tau \in \langle p, t \rangle$, then $P_i^{(\tau, p)}(s) = 1$; in particular $P_i^{(\sigma)}(s) = 1$ whenever $\langle p, t \rangle \subseteq \pi$. This implies

$$H(s) = \begin{cases} \prod_{i \in I_m} P_i^{(p)}(s) & \text{in cases (1) and (3) ,} \\ \prod_{i \in I_u, m \leq u \leq 5} P_i^{(2)}(s) & \text{otherwise.} \end{cases}$$

- Assume that (3) occurs and let $\tau \in \langle p, m \rangle$ exist. By Corollary 2.2.9 and Proposition 3.1.11, if $i \in I_m$, and there exists y such that $(p, y) = 1$ and $b_{i,y} \neq 0$ then $y = x^{r_i}$ and $v_\tau(x) = v_\tau(p^m - 1)$. Let

$$w = \min\{x \in \mathbb{N} : v_\tau(x) = v_\tau(p^m - 1) \text{ and } b_{i,x^{r_i}} \neq 0 \text{ for some } i \in I_m\}.$$

By Proposition 3.1.11, for each $i \in I_m$, if $b_{i,w^{r_i}} \neq 0$ then $b_{i,w^{r_i}} < 0$. Moreover, if $b_{i,w^{r_i}} \neq 0$ and $X_j \cong X_i$, then $b_{j,w^{r_j}} \neq 0$, so the set $\Sigma_m = \{i \in I_m \mid b_{i,w^{r_i}} \neq 0\}$ is infinite. Applying Proposition 2.4.3, we obtain a rational product

$$H^*(s) = \prod_{i \in \Sigma_m} \left(1 + \frac{b_{i,w^{r_i}}}{w^{r_i s}}\right), \text{ where } b_{i,w^{r_i s}} < 0 \text{ for all } i \in \Sigma_m. \tag{3.3}$$

By Corollary 2.5.5, the product $H^*(s)$ is a finite product, i.e., Σ_m is finite, which is a contradiction.

- Assume that (1) occurs. By Table 3.2, if $\zeta_p(S)=1$, then $S \cong \mathrm{PSL}(2,p)$. This implies in particular that
$$H(s)=\prod_{i\in I_1}\left(1-\frac{2^{tr_i}}{2^{tr_i s}}\right).$$
Again by Corollary 2.5.5, we get that I_1 is finite, which is a contradiction.

- Finally assume that the case (2) occurs. By Table 3.2, if $\zeta_p(S)\leq 5$, then S is one of the following groups: $\mathrm{PSL}(6,2)$, $U(4,2)$, $\mathrm{PSp}(6,2)$, $P\Omega^+(8,2)$, $\mathrm{PSL}(3,4)$, $\mathrm{PSL}(5,2)$, $\mathrm{PSL}(4,2)$, $\mathrm{PSL}(3,2)$. The explicit description of the Dirichlet series $P^{(2)}_{X,S}(s)$ when $S\leq X\leq \mathrm{Aut}(S)$ and S is one of the simple groups in the previous list, is included in Appendix 1. Notice in particular that if $i\in\Lambda=\bigcup_{m\leq 5} I_m$ then $\pi(P_i^{(2)}(s))\subseteq\{3,7,5,31\}$. First consider $\Lambda_{31}=\{i\in\Lambda \mid 31\in\pi(P_i^{(2)}(s))\}$ and let
$$\begin{aligned} w &= \min\{x\in\mathbb{N}\mid x \text{ is odd}, v_{31}(x)=1 \text{ and } b_{i,x^{r_i}}\neq 0 \text{ for some } i\in\Lambda\}\\ &= \min\{x\in\mathbb{N}\mid x \text{ is odd}, v_{31}(x)=1 \text{ and } b_{i,x^{r_i}}\neq 0 \text{ for some } i\in\Lambda_{31}\}\end{aligned}$$

Note that if $i\in\Lambda_{31}$ and n is minimal with the properties that n is odd, $b_{i,n^{r_i}}\neq 0$ and $v_{31}(n)=1$, then $b_{i,n^{r_i}}<0$ (see Appendix 1). So if $b_{i,w^{r_i}}\neq 0$ then $b_{i,w^{r_i}}<0$; moreover, by applying Proposition 2.4.3 we obtain a rational product
$$H^*(s)=\prod_{i\in\Lambda}\left(1+\frac{b_{i,w^{r_i}}}{w^{r_i s}}\right)=\prod_{i\in\Lambda_{31}}\left(1+\frac{b_{i,w^{r_i}}}{w^{r_i s}}\right), \text{ where } b_{i,w^{r_i}}\leq 0 \text{ for all } i\in\Lambda_{31}.$$
By Corollary 2.5.5, the set $\Lambda^*_{31}=\{i\in\Lambda_{31}\mid b_{i,w^{r_i}}\neq 0\}$ is finite, but this implies that $\Lambda_{31}=\emptyset$. Indeed, if $\Lambda_{31}\neq 0$, then there exists at least one index i with $i\in\Lambda^*_{31}$. Moreover, by assumption, there are infinitely many j with $X_j\cong X_i$ and all of them belong to Λ^*_{31}. Since $\Lambda_{31}=\emptyset$, if $i\in\Lambda$, then S_i is isomorphic to one of the following: $U(4,2), \mathrm{PSp}(6,2), P\Omega^+(8,2), \mathrm{PSL}(3,4), \mathrm{PSL}(4,2), \mathrm{PSL}(3,2)$. It follows from Appendix 1, that if $i\in\Lambda$, x is odd and $b_{i,x^{r_i}}\neq 0$, then $v_7(x)\leq 1$. But then, we may repeat the same argument as above and consider $\Lambda_7=\{i\in\Lambda\mid 7\in\pi(P_i^{\{2\}}(s))\}$ and
$$w:=\min\{x\in\mathbb{N}\mid x \text{ is odd}, v_7(x)=1 \text{ and } b_{i,x^{r_i}}\neq 0 \text{ for some } i\in\Lambda_7\}.$$

Arguing as before we deduce that $\Lambda_7=\emptyset$. We can see from Appendix 1 that this implies $S_i\cong U(4,2)$ for all $i\in\Lambda$ and
$$H^{\{5\}}(s)=\prod_{i\in\Lambda}\left(1-\frac{3^{3r_i}}{3^{3r_i s}}\right).$$

Again, by Corollary 2.5.5, Λ is finite and consequently $\Lambda = \emptyset$.

□

Appendix 1: exceptional cases

In this section, we give explicit formulas for $P^{(2)}_{X,S}(s)$ when X is an almost simple group whose socle S is of Lie type over a field of characteristic 2 and $\zeta_2(S) \leq 5$ (see Example 1 and Example 2 in Section 3 for the illustration of computation).

(i) $S = \mathrm{PSL}(6,2)$. If X contains a graph automorphism then

$$\begin{aligned} P^{(2)}_{X,S}(s) &= 1 - (3^2.7.31)^{(1-s)} - (3.5.7^2.31)^{(1-s)} - (3^3.7.31)^{(1-s)} \\ &+ 2(3^4.7^2.31)^{(1-s)} + (3^3.5.7^2.31)^{(1-s)} - (3^4.5.7^2.31)^{(1-s)}. \end{aligned}$$

If X does not contain graph automorphisms, then

$$\begin{aligned} P^{(2)}_{X,S}(s) &= 1 - 2(3^2.7)^{(1-s)} - (3^2.5.31)^{(1-s)} - 2(3.7.31)^{(1-s)} \\ &+ 3(3^2.7.31)^{(1-s)} + 6(3^2.5.7.31)^{(1-s)} + (3.5.7^2.31)^{(1-s)} \\ &- 4(3^3.5.7.31)^{(1-s)} - 6(3^2.5.7^2.31)^{(1-s)} \\ &+ 5(3^3.5.7^2.31)^{(1-s)} - (3^4.5.7^2.31)^{(1-s)}. \end{aligned}$$

(ii) $S = \mathrm{PSL}(5,2)$. If X contains a graph automorphism then

$$P^{(2)}_{X,S}(s) = 1 - (3.5.31)^{(1-s)} - (3^2.7.31)^{(1-s)} + (3^2.5.7.31)^{(1-s)}.$$

If X does not contain graph automorphisms, then

$$\begin{aligned} P^{(2)}_{X,S}(s) &= 1 - 2(31)^{(1-s)} - 2(5.31)^{(1-s)} + 3(3.5.31)^{(1-s)} \\ &+ 3(5.7.31)^{(1-s)} - 4(3.5.7.31)^{(1-s)} + (3^2.5.7.31)^{(1-s)}. \end{aligned}$$

(iii) $S = \mathrm{PSL}(4,2)$. If X contains a graph automorphism then

$$P^{(2)}_{X,S}(s) = 1 - (3^2.7)^{(1-s)} - (3.5.7)^{(1-s)} + (3^2.5.7)^{(1-s)}.$$

If X does not contain graph automorphisms, then

$$P^{(2)}_{X,S}(s) = 1 - 2(3.5)^{(1-s)} - (5.7)^{(1-s)} + 3(3.5.7)^{(1-s)} - (3^2.5.7)^{(1-s)}.$$

(iv) $S = \mathrm{PSL}(3,2)$. If X contains a graph automorphism then

$$P^{(2)}_{X,S}(s) \quad = \quad 1 - (3.7)^{(1-s)}.$$

If X does not contain graph automorphisms, then

$$P^{(2)}_{X,S}(s) \quad = \quad 1 - 2(7)^{(1-s)} + (3.7)^{(1-s)}.$$

(v) $S = \mathrm{PSL}(3,4)$. If X contains a graph automorphism then

$$P^{(2)}_{X,S}(s) = 1 - (3.5.7)^{(1-s)}.$$

If X does not contain graph automorphisms then

$$P^{(2)}_{X,S}(s) = 1 - 2(3.7)^{(1-s)} + (3.5.7)^{(1-s)}.$$

(vi) $S = \mathrm{PSp}(6,2)$. We have

$$P^{(2)}_{X,S}(s) = 1 - (3^2.7)^{(1-s)} - (3^3.5)^{(1-s)} - (3^2.5.7)^{(1-s)} + 3(3^3.5.7)^{(1-s)} - (3^4.5.7)^{(1-s)}.$$

(vii) $S = \mathrm{U}(4,2)$. We have

$$P^{(2)}_{X,S}(s) = 1 - (3^3)^{(1-s)} - (3^2.5)^{(1-s)} + (3^3.5)^{(1-s)}.$$

(viii) $S = \mathrm{P}\Omega^+(8,2)$. We have

$$\begin{aligned} P^{(2)}_{X,S}(s) &= 1 - 3(3^2.5)^{(1-s)} - (3.5^2.7)^{(1-s)} + 3(3^3.5^2)^{(1-s)} + 3(3^3.5^2.7)^{(1-s)} \\ &- 4(3^4.5^2.7)^{(1-s)} + (3^5.5^2.7)^{(1-s)}. \end{aligned}$$

Lie notation	Other notation	Conditions
$A_n(t)$	$\mathrm{PSL}(n+1,q)$	$n \geq 1, (n,t) \neq (1,2), (1,3)$
${}^2A_n(t^2)$	$\mathrm{PSU}(n+1,q)$	$n \geq 2, (n,t) \neq (2,2)$
$B_n(t)$	$\mathrm{P}\Omega(2n+1,q)$	$n \geq 3, t$ odd
${}^2B_2(t^2)$		$q = t^2 = 2^{2k+1}, k \geq 1$
$C_n(t)$	$\mathrm{PSp}(2n,q)$	$n \geq 2, (n,t) \neq (2,2)$
$D_n(t)$	$\mathrm{P}\Omega^+(2n,q)$	$n \geq 4$
${}^2D_n(t^2)$	$\mathrm{P}\Omega^-(2n,q)$	$n \geq 4$
${}^3D_4(t^3)$		
$E_6(t)$		
${}^2E_6(t^2)$		
$E_7(t)$		
$E_8(t)$		
$F_4(t)$		$t \geq 3$
${}^2F_4(t^2)$		$q = t^2 = 2^{2k+1}, k \geq 1$
$G_2(t)$		$t \geq 3$
${}^2G_2(t^2)$		$q = t^2 = 3^{2k+1}, k \geq 1$

Table 3.3: Classification of simple groups of Lie type

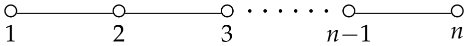
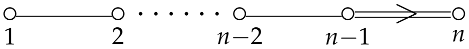
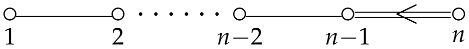
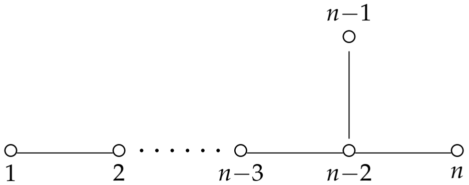
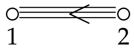
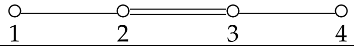
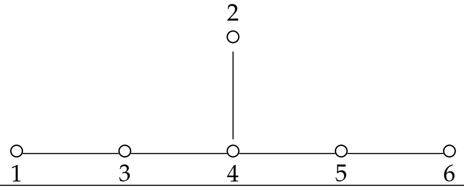
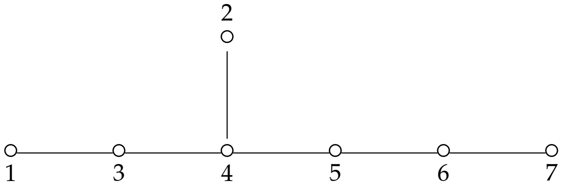
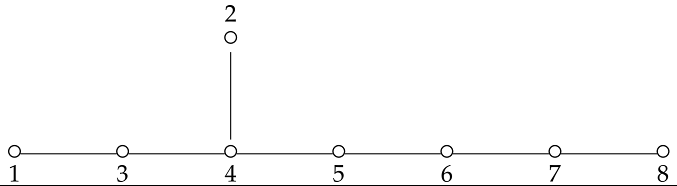
Lie notation	Dynkin diagram
$A_n, n \geq 1$	
$B_n, n \geq 2$	
$C_n, n \geq 3$	
$D_n, n \geq 4$	
G_2	
F_4	
E_6	
E_7	
E_8	

Table 3.4: The classification of simple Lie algebras

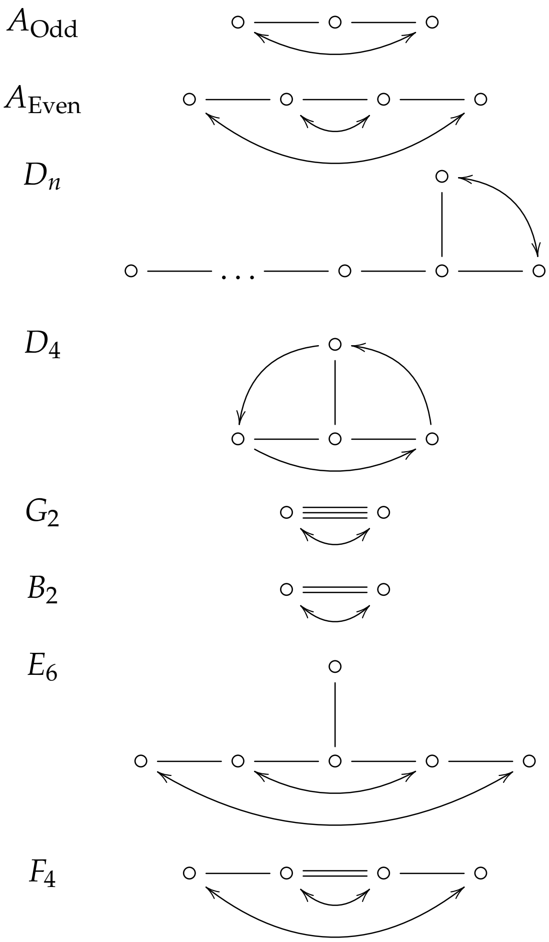


Table 3.5: Symmetries of Dynkin diagrams

Chapter 4

Linear groups of dimension two

This chapter is devoted for a proof of **Theorem B** as the following.

Theorem B. *Let G be a finitely generated profinite group such that almost every nonabelian composition factor is isomorphic to $PSL(2,p)$ for some prime $p \geq 5$. Then $P_G(s)$ is rational only if $G/\mathrm{Frat}(G)$ is finite.*

4.1 Maximal subgroups of PSL$(2,q)$

Let X be an almost simple group with socle $S \cong \mathrm{PSL}(2,q)$ where $q \geq 5$ is a prime. Since $\mathrm{Aut}(S) = \mathrm{PGL}(2,q)$ and $|\mathrm{PGL}(2,q) : \mathrm{PSL}(2,q)| = 2$, either $X = \mathrm{PSL}(2,q)$ or $X = \mathrm{PGL}(2,q)$. We will now look for the smallest index of maximal subgroups supplementing S in X that is divisible by q and not divisible by 2.

Theorem 4.1.1 ([Dic58]). *Let $X = PGL(2,q)$ with $q \geq 5$ a prime. Then the maximal subgroups of X not containing $PSL(2,q)$ are*

(a) $C_q \rtimes C_{q-1}$;

(b) $D_{2(q-1)}$ *for* $q \neq 5$;

(c) $D_{2(q+1)}$;

(d) $Sym(4)$ *for* $q \equiv \pm 3 \mod 8$.

We list those maximal subgroups of $\mathrm{PGL}(2,q)$ and their indices in the following table:

maximal subgroup	order	index
$C_q \rtimes C_{q-1}$	$q(q-1)$	$q+1$
$D_{2(q-1)}, q \neq 5$	$2(q-1)$	$q(q+1)/2$
$D_{2(q+1)}$	$2(q+1)$	$q(q-1)/2$
$\mathrm{Sym}(4), q \equiv \pm 3 \mod 8$	$4!$	$q(q^2-1)/4!$

Table 4.1: Maximal subgroups of $\mathrm{PGL}(2,q)$

We consider indices divisible by q.

- Assume that $q(q-1)/2$ is odd. If there exists a maximal subgroup M such that $|\mathrm{PGL}(2,q) : M|$ is odd and smaller than $q(q-1)/2$, then $M \cong \mathrm{Sym}(4)$. In this case, $q \equiv \pm 3 \mod 8$, and we have

$$\frac{q(q^2-1)}{4!} < \frac{q(q-1)}{2} \Leftrightarrow q < 11$$

  so $q = 5$. For $q = 5$, we have $q(q^2-1)/4! = 5$, while $q(q-1)/2 = 10$ and $q(q+1)/2 = 15$.

- Assume now that $q(q+1)/2$ is odd. If there exists a maximal subgroup M such that $|\mathrm{PGL}(2,q) : M|$ is odd and smaller than $q(q-1)/2$, then $M \cong \mathrm{Sym}(4)$. Also in this case, $q \equiv \pm 3 \mod 8$, and we have

$$\frac{q(q^2-1)}{4!} < \frac{q(q+1)}{2} \Leftrightarrow q < 12$$

  The candidates are $q = 5 \equiv 1 \mod 4$ and $q = 11 \equiv 3 \mod 4$. The case $q = 5$ was already eliminated above. In the case $q = 11$, we choose index $q(q-1)/2 = 55$ which is not divisible by 2.

Theorem 4.1.2 ([Dic58]). *Let $X = PSL(2,q)$ with $q \geq 5$ a prime. Then the maximal subgroups of X are the following*

(a) $C_q \rtimes C_{q-1}$*;*

(b) D_{q-1} *for* $q \geq 13$*;*

(c) D_{q+1} *for* $q \neq 7, 9$*;*

(d) $Sym(4)$ *for* $q \equiv \pm 1 \mod 8$*;*

(e) $Alt(4)$ *for* $q \equiv \pm 3 \mod 10$

(f) $Alt(5)$ *for* $q \equiv \pm 1 \mod 10$*.*

We have a table of maximal subgroups of $\mathrm{PSL}(2, q)$ and their indices as follows.

maximal subgroup M	order	index
$C_q \rtimes C_{q-1}$	$q(q-1)$	$q+1$
$D_{(q-1)}, q \geq 13$	$2(q-1)$	$q(q+1)/2$
$D_{(q+1)}, q \neq 7, 9$	$2(q+1)$	$q(q-1)/2$
$\mathrm{Sym}(4)$, $q \equiv \pm 1 \mod 8$	$4!$	$q(q^2-1)/2.4!$
$\mathrm{Alt}(4), q \equiv \pm 3 \mod 10$ & $q \not\equiv \pm 1 \mod 10$	$4!/2$	$q(q^2-1)/4!$
$\mathrm{Alt}(5), q \equiv \pm 1 \mod 10$	$5!/2$	$q(q^2-1)/5!$

Table 4.2: Maximal subgroups of $\mathrm{PSL}(2, q)$

We look for the smallest odd integer divisible by q which is the index of a maximal subgroup M of $\mathrm{PSL}(2, q)$. We have two cases:

(a) If $q(q-1)/2$ is odd, then either $|\mathrm{PSL}(2, q) : M| = q(q-1)/2$ or one of the following cases occurs:

In case $M = \mathrm{Alt}(4)$ with $q \equiv \pm 3 \mod 10$, we have

$$\frac{q(q^2-1)}{4!} < \frac{q(q-1)}{2} \Leftrightarrow q < 11.$$

The only candidate is $q = 5 \equiv 1 \mod 4$. For $q = 5$ we have $q(q^2-1)/4! = 5$, while $q(q-1)/2 = 10$, and $q(q+1)/2 = 15$.

In case $M = \mathrm{Sym}(4)$ with $q \equiv \pm 1 \mod 8$, we have

$$\frac{q(q^2-1)}{2.4!} < \frac{q(q-1)}{2} \Leftrightarrow q < 23.$$

The only candidate is $q = 7 \equiv 3 \mod 4$. For $q = 7$ we have $q(q^2-1)/2.4! = 7$, while $q(q-1)/2 = 21$.

In case $M = \mathrm{Alt}(5)$ with $q \equiv \pm 1 \mod 10$, we have

$$\frac{q(q^2-1)}{5!} < \frac{q(q-1)}{2} \Leftrightarrow q < 59.$$

The candidates are $q = 11 \equiv 3 \mod 4$, $q = 19 \equiv 3 \mod 4$, $q = 29 \equiv 1 \mod 4$, $q = 31 \equiv 3 \mod 4$, $q = 41 \equiv 1 \mod 4$, $q = 49 \equiv 1 \mod 4$.

For $q = 11$ we have $q(q^2-1)/5! = 11$ while $q(q-1)/2 = 55$.
For $q = 19$ we have $q(q^2-1)/5! = 19 \cdot 3$ while $q(q-1)/2 = 19 \cdot 9$.
For $q = 29$ we have $q(q^2-1)/5! = 29 \cdot 7$ while $q(q-1)/2 = 29 \cdot 14$.
For $q = 31$ we have $q(q^2-1)/5! = 31 \cdot 8$ while $q(q-1)/2 = 31 \cdot 15$.
For $q = 41$ we have $q(q^2-1)/5! = 41 \cdot 14$ while $q(q-1)/2 = 41 \cdot 20$.
For $q = 49$ we have $q(q^2-1)/5! = 49 \cdot 20$ while $q(q-1)/2 = 49 \cdot 24$.

(b) If $q(q+1)/2$ is odd, then, similarly, either $|\mathrm{PSL}(2,q) : M| = q(q+1)/2$ or one of the following cases occurs:

In case $M = \mathrm{Alt}(4)$ with $q \equiv \pm 3 \mod 10$ and $q \not\equiv \pm 1 \mod 10$, we have

$$\frac{q(q^2-1)}{4!} < \frac{q(q+1)}{2} \Leftrightarrow q < 13.$$

Candidates are $q = 5 \equiv 1 \mod 4$ and $q = 11 \equiv 3 \mod 4$ which are already eliminated above.

In case $M = \mathrm{Sym}(4)$ with $q \equiv \pm 1 \mod 8$, we have

$$\frac{q(q^2-1)}{2.4!} < \frac{q(q+1)}{2} \Leftrightarrow q < 25.$$

The remaining candidate is $q = 23 \equiv 3 \mod 4$. But in this case, we choose $q(q-1)/2 = 23 \cdot 11$ instead of $q(q+1)/2 = 23 \cdot 12$.

In case $M = \mathrm{Alt}(5)$ with $q \equiv \pm 1 \mod 10$, we have

$$\frac{q(q^2-1)}{5!} < \frac{q(q+1)}{2} \Leftrightarrow q < 61.$$

The remaining candidate is $q = 59 \equiv 3 \mod 4$. Again, in this case, we choose $q(q-1)/2 = 59 \cdot 29$ instead of $q(q+1)/2 = 59 \cdot 30$.

Theorem 4.1.3. *Let L be a monolithic primitive group with $\mathrm{soc}(L) = (PSL(2,q))^r$ for some prime $q \geq 5$, and X the associated almost simple group. Define w as follows :*

$$w = w(X) = \begin{cases} q(q-1)/2 & \textit{if } q \equiv 3 \mod 4 \textit{ and } q \notin \{5,7,11,19,29\}, \\ q(q+1)/2 & \textit{if } q \equiv 1 \mod 4 \textit{ and } q \notin \{5,7,11,19,29\}, \\ 5 & \textit{if } q = 5, \\ 7 & \textit{if } q = 7 \textit{ and } X = PSL(2,7), \\ 3 \cdot 7 & \textit{if } q = 7 \textit{ and } X = PGL(2,7), \\ 11 & \textit{if } q = 11 \textit{ and } X = PSL(2,11), \\ 11 \cdot 5 & \textit{if } q = 11 \textit{ and } X = PGL(2,11), \\ 19 \cdot 3 & \textit{if } q = 19 \textit{ and } X = PSL(2,19), \\ 19 \cdot 3^2 & \textit{if } q = 19 \textit{ and } X = PGL(2,19), \\ 29 \cdot 7 & \textit{if } q = 29 \textit{ and } X = PSL(2,29), \\ 29 \cdot 3 \cdot 5 & \textit{if } q = 29 \textit{ and } X = PGL(2,29). \end{cases}$$

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

4.2 The main result

In this section, we give a proof for **Theorem B**. In this proof, we consider a finitely generated profinite group G such that $P_G(s)$ is rational and that there is an open normal subgroup H of which every composition factor is either cyclic or isomorphic to a group $\mathrm{PSL}(2,p)$ for some prime $p \geq 5$.

We fix a descending normal series $\{G_i\}$ of G with the properties that $\bigcap G_i = 1$ and G_i/G_{i+1} is a chief factor of G/G_{i+1}. Let J be the set of indices i with G_i/G_{i+1} non-Frattini. Then by Section 2.1 the probabilistic zeta function $P_G(s)$ can be factorized as

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

where for each i, the finite Dirichlet series $P_i(s) = \sum_n b_{i,n}/n^s$ is associated to the chief factor G_i/G_{i+1}. We have the the following crucial result.

Proposition 4.2.1. *The set $\pi(G)$ is finite.*

Proof. Let Γ be 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 $i \in J$. Since $P_G(s)$ is rational, the set $\pi(P_G(s))$ is finite. Therefore, it follows from Lemma 2.6.1 that Γ contains only finitely many abelian groups. Assume by contradiction that Γ is infinite. By our assumption, the subset Γ^* of the simple groups in Γ that are isomorphic to $\mathrm{PSL}(2,p)$ for some prime p is infinite. Let

$$I := \{j \in J \mid S_j \in \Gamma^*\},\ A(s) := \prod_{i \in I} P_i(s) \text{ and } B(s) := \prod_{i \notin I} P_i(s).$$

Notice that $\pi(B(s)) \subseteq \bigcup_{\in \Gamma \setminus \Gamma^*} \pi(S)$ is a finite set. Since $P_G(s) = A(s)B(s)$ and $\pi(P_G(s))$ is finite, if follows that the set $\pi(A(s))$ is finite. In particular, there exists a prime number $q \geq 5$ such that $q \notin \pi(A(s))$ but $\mathrm{PSL}(2,q) \in \Gamma^*$. Let Λ be the set of the odd integers n divisible by q but not divisible by any prime strictly greater than q and set

$$\begin{aligned}
&r := \min\{r_i \mid S_i = \mathrm{PSL}(2,q)\},\\
&I^* := \{i \in I \mid S_i = \mathrm{PSL}(2,q) \text{ and } r_i = r\},\\
&w := \min\{w(X_i) \mid S_i = \mathrm{PSL}(2,q) \text{ and } r_i = r\},\\
&\alpha := \min\{n > 1 \mid n \in \Lambda, v_q(n) = r \text{ and } b_{i,n} \neq 0 \text{ for some } i \in I\}.
\end{aligned}$$

Assume $i \in I$, $n \in \Lambda$ and $b_{i,n} \neq 0$. We have that $S_i \cong \mathrm{PSL}(2,q_i)$ for a suitable prime q_i. Since $b_{i,n} \neq 0$, there is a subgroup $H \leq L_i$ such that $L_i = H \cdot \mathrm{soc}(L_i)$ and $n = [L_i : H]$. Hence $n = |L_i : H| = |\mathrm{soc}(L_i) : \mathrm{soc}(L_i) \cap H|$. Since $q|n$, and q_i is the largest prime divisor of $|S_i| = |\mathrm{PSL}(2,q_i)| = q_i(q_i^2-1)/2$, we get that $q_i \geq q$. Since n is an odd useful index for L_i, we have by Lemma 2.2.6 that $n = x^{r_i}$, where x is an odd useful index for the almost simple group X_i where $\mathrm{soc}(X_i) = S_i = \mathrm{PSL}(2,q_i)$. So, there is a maximal subgroup of X_i, which supplements S_i, of odd index x' dividing x. If $q_i > q$, then q_i does not divide n by definition of $n \in \Lambda$, so x' is not divisible by q_i. It means that X_i has a maximal subgroup of odd index divisible by q and not divisible by q_i, which contradicts the tables we have above. Hence $q_i = q$. It follows that $\alpha = w^r$ and $b_{i,\alpha} \neq 0$ if and only if $i \in I^*$ and $w(X_i) = w$; moreover in the last case $b_{i,\alpha} < 0$. Hence the coefficient c_α of $1/c_\alpha$ in $A(s)$ is

$$c_\alpha = \sum_{i \in I^*, w(X_i) = w} b_{i,\alpha} < 0.$$

This implies that $q \in \pi(A(s))$, which is a contradiction. Thus Γ^*, and hence Γ, is finite. By Corolary 2.6.2, it follows that $\pi(G)$ is also finite. □

Proof of Theorem B. Assume that $P_G(s) = \prod_{i \in J} P_i(s)$ where J is the set of indices i such that G_i/G_{i+1} is non-Frattini. Let $\mathcal{T}$ be the set of almost simple groups X such that there exist infinitely many $i \in J$ with $X_i \cong X$ and let I be the set of indices $i \in J$ such that $X_i \in \mathcal{T}$. By Proposition 2.6.3, the set $J \setminus I$ is finite. We have to prove that J is finite; this is equivalent to show that $I = \emptyset$. Assume that $I \neq \emptyset$ and let $i \in I$. By the hypothesis of Theorem B, there exists a prime q_i such that $S_i \in \{C_{q_i}, \mathrm{PSL}(2, q_i)\}$. Set $q = \max\{q_i : i \in I\}$ and let Λ be the set of odd integers n divisible by q. Assume $n \in \Lambda$ and $b_{i,n} \neq 0$ for some $i \in I$. If S_i is cyclic, then $P_i(s) = 1 - c_n/n^s$ where $n = |G_i/G_{i+1}| = q_i^{r_i}$ and c_n is the number of complements of G_i/G_{i+1} in G/G_{i+1}. This implies $q = q_i$ and $v_q(n) = r_i$. If $S_i = \mathrm{PSL}(2, q_i)$, then by the proof of Proposition 4.2.1, we have $q_i \geq q$, and by the maximality of q, we obtain that $q_i = q$. In addition, n is an odd useful index for L_i, so, by Lemma 2.2.6, we have $n = x_i^{r_i}$, where x_i is an odd useful index of a subgroup Y_i supplementing S_i in the almost simple group X_i with $\mathrm{soc}(X_i) = S_i$. Since $q | n = x_i^{r_i}$, then $q | x_i$, so $v_q(x_i) \geq 1$. Since $q_i = q$ and q_i^2 does not divide the order of X_i, we obtain $v_q(x_i) = 1$, hence $v_q(n) = r_i$. Let

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

Since $J \setminus I$ is finite and $P_G(s) = \prod_{i \in J} P_i(s)$ is rational, also $\prod_{i \in I} P_i(s)$ is rational. This implies by Lemma 1.2.5 that the product $Q(s) = \prod_i P_i^{(2)}(s)$ is also rational. Let $I^* = \{i \in I \mid b_{i,w^{r_i}} \neq 0\}$. By the above considerations and Theorem 4.1.3, we have $i \in I^*$ if and only if either $S_i \cong C_q$ and $w = q$ or $\mathrm{soc}(X_i) = \mathrm{PSL}(2, q)$ and $w_i = w$. In particular, if $i \in I^*$ then there exist infinitely many $j \in I$ with $X_i \cong X_j$ and all of them are in I^*, hence I^* is an infinite set. Moreover, $b_{i,w^{r_i}} < 0$ for every $i \in I^*$, and therefore applying Proposition 2.4.3 to the Dirichlet series $Q(s)$, we deduce that the product

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

is rational. By Corollary 2.5.5, the set I^* must be finite, a contradiction. □

Chapter 5

Sporadic simple groups

This chapter is devoted for a proof of **Theorem C** as the following.

Theorem C. *If G is a finitely generated profinite group such that almost every nonabelian composition factor is isomorphic to a sporadic simple group and $P_G(s)$ is rational, then $G/\mathrm{Frat}(G)$ is a finite group.*

The list of sporadic simple groups with their orders and automorphism groups is described in Table 5.1.

Note that if X is an almost simple group whose socle S is a sporadic group, then either $X = S$ or $X = S \cdot 2$. If $X = S$ then $P_{X,S}(s) = P_S(s)$. If $X = S \cdot 2$ then $X/S \cong C_2$, and so

$$P_X(s) = P_{X,S}(s)P_{X/S}(s) = P_{X,S}(s)\left(1 - \frac{1}{2^s}\right)$$

which implies that $P^{(2)}_{X,S}(s) = P^{(2)}_X(s)$. This helps us analyse $P^{(2)}_{X,S}(s)$ easily from the knowledge of X. Therefore, we will focus only on odd indices of subgroups of X. Let Γ_X be the set of useful subgroups of X of odd index, and let $m_X = \min\{|X : H| : H \in \Gamma_X\}$. Then m_X is the index of a maximal subgroup of X. In order to apply our machinery, we need to look for a prime divisor p_X of m_X such that if p_X divides the index $|X : H|$ of some subgroup $H \in \Gamma_X$, then $v_{p_X}(m_X) = v_{p_X}(|X : H|)$. Notice also that for any prime $p \in \pi(m_X)$, if there is some $H \in \Gamma_X$ such that $p||X : H|$, then $m_X \leq |X : H|$. The list of m_X and all potential p_X for all sporadic groups is included in Table 5.3.

Proof of Theorem C. Since there are only 26 sporadic simple groups, by Step 1 in Section 2.6, the set $\pi(G)$ is finite. We have that

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

where J is the set of indices i with G_i/G_{i+1} non-Frattini. Let $\mathcal{T}$ be the set of almost simple groups X such that $\mathrm{soc}(X)$ is a sporadic simple group and there exist infinitely many $i \in J$ with $X_i \cong X$, and let $I = \{i \in J \mid X_i \in \mathcal{T}\}$. By Proposition 2.6.3, the set $J \setminus I$ is finite. We have to prove that J is finite; this is equivalent to showing that $I = \emptyset$. For any almost simple group X, let $\Omega(X)$ be the set of the odd integers $m \in \mathbb{N}$ such that:

- X contains at least one subgroup Y such that $X = Y \cdot \mathrm{soc}(X)$ and $|X : Y| = m$.

- if $X = Y \cdot \mathrm{soc}(X)$ and $|X : Y| = m$, then Y is a maximal subgroup of X.

Note that if $m \in \Omega(X)$, $X = Y \cdot \mathrm{soc}(X)$ and $|X : Y| = m$, then $\mu_X(Y) = -1$; in particular, $b_m(X) < 0$. This implies that if $m \in \Omega(X_i)$ then $b_{i,m^{r_i}} < 0$. Certainly $\Omega(X)$ is not empty and its smallest element is the smallest index m_X of a supplement of $\mathrm{soc}(X)$ in X (see Table 5.3). In a few cases, we need to know another integer n_X in $\Omega(X)$, given in Table 5.4.

Since $J \setminus I$ is finite and $P_G(s) = \prod_{i \in J} P_i(s)$ is rational, also $\prod_{i \in I} P_i(s)$ is rational. This implies from Lemma 1.2.5 that the product $Q(s) = \prod_{i \in I} P_i^{(2)}(s)$ is also rational. For a fixed prime p, let $\Lambda_p = \{i \in I \mid p \in \pi(P_i^{\{2\}}(s))\}$.

If $i \in \Lambda_{31}$, then 31 divides $|S_i|$ and $S_i \in \{\mathrm{J}_4, \mathrm{Ly}, \mathrm{O'N}, \mathrm{BM}, \mathrm{M}, \mathrm{Th}\}$. Moreover 31^2 does not divide $|S_i|$ so if n is odd, divisible by 31 and $b_{i,n} \neq 0$ then $n = x^{r_i}$ and $v_{31}(x) = 1$. Let $m_i = n_{X_i}$ if $S_i \cong \mathrm{Th}$, and $m_i = m_{X_i}$ otherwise. Since m_i is the smallest odd number divisible by 31 and equal to the index in X_i of a supplement of S_i we get:

$$\begin{aligned} w &= \min\{x \in \mathbb{N} \mid x \text{ is odd }, v_{31}(x) = 1 \text{ and } b_{i,x^{r_i}} \neq 0 \text{ for some } i \in I\} \\ &= \min\{x \in \mathbb{N} \mid x \text{ is odd }, v_{31}(x) = 1 \text{ and } b_{i,x^{r_i}} \neq 0 \text{ for some } i \in \Lambda_{31}\} \\ &= \min\{m_i \mid i \in \Lambda_{31}\}. \end{aligned}$$

But then by Proposition 2.4.3, the following Dirichlet series is rational:

$$\prod_{i \in \Lambda_{31}} \left(1 + \frac{b_{i,w^{r_i}}}{(w^{r_i})^s}\right).$$

We have $b_{i,w^{r_i}} < 0$ if $m_i = w$, $b_{i,w^{r_i}} = 0$ otherwise. By applying Corollary 2.5.5, we get that $\{i \in \Lambda_{31} \mid m_i = w\}$ is a finite set, and this implies $\Lambda_{31} = \emptyset$.

Now consider Λ_{23}. Since $\Lambda_{31} = \emptyset$, if $i \in \Lambda_{23}$ then $S_i \in \{\mathrm{M}_{23}, \mathrm{M}_{24}, \mathrm{Co}_1, \mathrm{Co}_2, \mathrm{Co}_3, \mathrm{Fi}_{23}, \mathrm{Fi}_{24}{}'\}$. We can repeat the argument used to proved that $\Lambda_{31} = \emptyset$. Let $m_i = n_{X_i}$ if $S_i \cong \mathrm{Co}_1$, $m_i = m_{X_i}$ otherwise and let $w = \min\{m_i \mid i \in \Lambda_{23}\}$. By applying Corollary 2.5.5, we get that $\{i \in \Lambda_{23} \mid m_i = w\}$ is a finite set, and this implies $\Lambda_{23} = \emptyset$.

New we consider Λ_{11}. Since $\Lambda_{31} \cup \Lambda_{23} = \emptyset$, if $i \in \Lambda_{11}$, then $S_i \in \{\mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{M}_{22}, \mathrm{J}_1,$ HS, Suz, McL, HN, $\mathrm{Fi}_{22}\}$. Let $m_i = n_{X_i}$ if $S_i \cong \mathrm{Fi}_{22}$ or $S_i \cong \mathrm{Fi}_{24}'$, $m_i = m_{X_i}$ otherwise and let $w = \min\{m_i \mid i \in \Lambda_{11}\}$. As before, by applying Corollary 2.5.5, we get that $\{i \in \Lambda_{23} \mid m_i = w\}$ is a finite set, and this implies $\Lambda_{11} = \emptyset$. Continuing our procedure, we consider Λ_{17}: if $i \in \Lambda_{17}$, then $S_i \in \{\mathrm{J}_3, \mathrm{He}\}$ and we can take $w = \min\{m_{X_i} \mid i \in \Lambda_{17}\}$ and deduce that $\Lambda_{17} = \emptyset$. Next we take $w = m_X$ with $\mathrm{soc}(X) = \mathrm{Ru}$ to prove $\Lambda_{29} = \emptyset$ and finally we take $w = m_X$ with $\mathrm{soc}(X) = \mathrm{J}_2$ to prove $\Lambda_7 = \emptyset$. In conclusion, the set

$$I = \Lambda_{31} \cup \Lambda_{23} \cup \Lambda_{11} \cup \Lambda_{29} \cup \Lambda_{17} \cup \Lambda_7$$

is empty, the Theorem follows. □

Tables

Table 5.1: Sporadic simple groups

S	$\|\mathrm{Out}(S)\|$	$\|S\|$
M_{11}	1	$2^4 \cdot 3^2 \cdot 5 \cdot 11$
M_{12}	2	$2^6 \cdot 3^3 \cdot 5 \cdot 11$
M_{22}	2	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$
M_{23}	1	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
M_{24}	1	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
J_1	1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
J_2	2	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$
J_3	2	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$
J_4	1	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$
HS	2	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$
Suz	2	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
McL	2	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$
Ru	1	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$

He	2	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$
Ly	1	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$
O′N	2	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$
Co_1	1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$
Co_2	1	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Co_3	1	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Fi_{22}	2	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
Fi_{23}	1	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$
Fi_{24}'	2	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
HN	2	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$
Th	1	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$
BM	1	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$
M	1	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 59 \cdot 71$

Table 5.2: Maximal subgroups of odd index of sporadic groups and their automorphism groups

Group	Maximal subgroup	Index
M_{11}	$M_{10} \cong A_6 \cdot 2$	11
	$M_9 : 2 \cong 3^2 : Q_8 \cdot 2$	$5 \cdot 11$
	$M_8 : S_3 \cong 2 \cdot S_4$	$3 \cdot 5 \cdot 11$
M_{12}	$M_8 \cdot S_4 \cong 2^{1+4} \cdot S_3$	$3^2 \cdot 5 \cdot 11$
	$4^2 : D_{12}$	$3^2 \cdot 5 \cdot 11$
$M_{12} \cdot 2$	$2^{1+4} \cdot S_3 : 2$	$3^2 \cdot 5 \cdot 11$
	$4^2 : D_{12} \cdot 2$	$3^2 \cdot 5 \cdot 11$
M_{22}	$2^4 : A_6$	$7 \cdot 11$
	$2^4 : S_5$	$3 \cdot 7 \cdot 11$
$M_{22} \cdot 2$	$2^4 : A_6 : 2$	$7 \cdot 11$
	$2^5 : S_5$	$3 \cdot 7 \cdot 11$
M_{23}	M_{22}	23
	$PSL(3,4) : 2$	$11 \cdot 23$
	$2^4 : A_7$	$11 \cdot 23$
	$2^4 : (3 \times A_5) : 2$	$7 \cdot 11 \cdot 23$
M_{24}	$2^4 \cdot A_8$	$3 \cdot 11 \cdot 23$
	$(2^6 \cdot 3) \cdot S_6$	$7 \cdot 11 \cdot 23$
	$2^6 \cdot (S_3 \times PSL(2,7))$	$3 \cdot 5 \cdot 11 \cdot 23$
J_1	$2^3 : 7 : 3$	$5 \cdot 11 \cdot 19$
	$2 \times A_5$	$7 \cdot 11 \cdot 19$

J_2	$2^{1+4} : A_5$ $2^{2+4} : (3 \times S_3)$	$3^2 \cdot 5 \cdot 7$ $3 \cdot 5^2 \cdot 7$
$J_2 \cdot 2$	$2^{1+4} \cdot A_5 \cdot 2$ $2^{2+4} : (3 \times S_3) \cdot 2$	$3^2 \cdot 5 \cdot 7$ $3 \cdot 5^2 \cdot 7$
J_3	$2^{1+4} : A_5$ $2^{2+4} : (3 \times S_3)$	$3^4 \cdot 17 \cdot 19$ $3^3 \cdot 5 \cdot 17 \cdot 19$
$J_3 \cdot 2$	$2^{1+4} \cdot S_5$ $2^{2+4} : (S_3 \times S_3)$	$3^4 \cdot 17 \cdot 19$ $3^3 \cdot 5 \cdot 17 \cdot 19$
J_4	$2^{11} : M_{24}$ $2^{1+12} \cdot 3M_{22} : 2$ $2^{3+12} \cdot (S_5 \times PSL(3,2))$	$11^2 \cdot 29 \cdot 31 \cdot 37 \cdot 43$ $11^2 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$ $3 \cdot 11^2 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$
Co_1	$2^{11} : M_{24}$ $2^{1+8} \cdot O_8^+(2)$ $2^{2+12} : (A_8 \times S_3)$ $2^{4+12} \cdot (S_3 \times 3S_6)$	$3^6 \cdot 5^3 \cdot 7 \cdot 13$ $3^4 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 23$ $3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 13 \cdot 23$ $3^5 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$
Co_2	$2^{10} : M_{22} : 2$ $2^{1+8} : S_6(2)$ $2^{4+10} \cdot (S_5 \times S_3)$	$3^4 \cdot 5^2 \cdot 23$ $3^2 \cdot 5^2 \cdot 11 \cdot 23$ $3^4 \cdot 5^2 \cdot 7 \cdot 11 \cdot 23$
Co_3	$2 \cdot S_6(2)$ $2^4 \cdot A_8$ $2^2 \cdot [2^7 \cdot 3^2] \cdot S_3$	$3^3 \cdot 5^2 \cdot 11 \cdot 23$ $3^5 \cdot 5^2 \cdot 11 \cdot 23$ $3^4 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Ly	$3 \cdot \mathrm{McL} : 2$ $2 \cdot A_{11}$	$5^3 \cdot 31 \cdot 37 \cdot 67$ $3^3 \cdot 5^4 \cdot 31 \cdot 37 \cdot 67$
Th	$2^5 \cdot PSL(5,2)$ $2^{1+8} \cdot A_9$	$3^8 \cdot 5^2 \cdot 7 \cdot 13 \cdot 19$ $3^6 \cdot 5^2 \cdot 7 \cdot 13 \cdot 19 \cdot 31$
Suz	$2^{1+6} \cdot U_4(2)$ $3^5 : M_{11}$ $2^{4+6} : 3A_6$ $2^{2+8} : (A_5 \times S_3)$	$3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ $3^9 \cdot 5 \cdot 7 \cdot 13$ $3^4 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ $3^5 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
$\mathrm{Suz} \cdot 2$	$2^{1+6} \cdot U_4(2) \cdot 2$ $3^5(M_{11} \times 2)$ $2^{4+6} : 3S_6$ $2^{2+8} : (S_5 \times S_3)$	$3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ $3^9 \cdot 5 \cdot 7 \cdot 13$ $3^4 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ $3^5 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
Fi_{22}	$2^{10} : M_{12}$ $(2 \times 2^{1+8} \cdot U_4(2)) : 2$ $2^{5+8} : (S_3 \times A_6)$	$3^7 \cdot 5 \cdot 13$ $3^5 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ $3^6 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
$\mathrm{Fi}_{22} \cdot 2$	$2^{10} : M_{12} : 2$ $(2 \times 2^{1+8} \cdot U_4(2) : 2) : 2$ $2^{5+8} : (S_3 \times S_6)$	$3^7 \cdot 5 \cdot 13$ $3^5 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ $3^6 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
Fi_{23}	$2 \cdot \mathrm{Fi}_{22}$	$3^4 \cdot 17 \cdot 23$

	$2^2 \cdot U_6(2) \cdot 2$	$3^7 \cdot 5 \cdot 13 \cdot 17 \cdot 23$
	$2^{11} \cdot M_{23}$	$3^{11} \cdot 5 \cdot 13 \cdot 17$
	$(2^2 \times 2^{1+8}) \cdot (3 \times U_4(2)) \cdot 2$	$3^8 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$
	$2^{6+8} : (A_7 \times S_3)$	$3^{10} \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot 23$
Fi_{24}'	$2^{11} \cdot M_{24}$	$3^{13} \cdot 5 \cdot 7^2 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
	$2^{1+12} \cdot 3U_4(2) \cdot 2$	$3^9 \cdot 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
	$2^{3+12} \cdot (PSL(3,2) \times A_6)$	$3^{13} \cdot 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
	$2^{6+8} \cdot (S_3 \times A_8)$	$3^{13} \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
$\mathrm{Fi}_{24}' \cdot 2$	$2^{12} \cdot M_{24}$	$3^{13} \cdot 5 \cdot 7^2 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
	$2^{1+12} \cdot 3U_4(2) \cdot 2^2$	$3^9 \cdot 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
	$2^{3+12} \cdot (PSL(3,2) \times S_6)$	$3^{13} \cdot 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
	$2^{7+8} \cdot (S_3 \times A_8)$	$3^{13} \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
O′N	$4 \cdot PSL(3,4) : 2$	$3^2 \cdot 7^2 \cdot 11 \cdot 19 \cdot 31$
	$4^3 \cdot PSL(2,31)$	$3^3 \cdot 5 \cdot 7^2 \cdot 11 \cdot 19 \cdot 31$
O′N.2	$4 \cdot PSL(3,4) : 2^2$	$3^2 \cdot 7^2 \cdot 11 \cdot 19 \cdot 31$
	$4^3 \cdot (PSL(2,31) \times 2)$	$3^3 \cdot 5 \cdot 7^2 \cdot 11 \cdot 19 \cdot 31$
Ru	$2^{3+8} : PSL(3,2)$	$3^2 \cdot 5^3 \cdot 13 \cdot 29$
	$2 \cdot 2^{4+6} : S_5$	$3^2 \cdot 5^2 \cdot 7 \cdot 13 \cdot 29$
He	$2^6 : 3 \cdot S_6$	$5 \cdot 7^3 \cdot 17$
	$2^{1+6} \cdot PSL(3,2)$	$3^2 \cdot 5^2 \cdot 7^2 \cdot 17$
He $\cdot$ 2	$2^{4+4} \cdot (S_3 \times S_3) \cdot 2$	$3 \cdot 5^2 \cdot 7^3 \cdot 17$
	$2^{1+6} \cdot PSL(3,2) \cdot 2$	$3^2 \cdot 5^2 \cdot 7^2 \cdot 17$
HS	$4^3 : PSL(3,2)$	$3 \cdot 5^3 \cdot 11$
	$4 \cdot 2^4 : S_5$	$3 \cdot 5^2 \cdot 7 \cdot 11$
HS $\cdot$ 2	$4^3 : (PSL(3,2) \times 2)$	$3 \cdot 5^3 \cdot 11$
	$2^{1+6} : S_5$	$3 \cdot 5^2 \cdot 7 \cdot 11$
McL	$U_4(3)$	$5^2 \cdot 11$
	M_{22}	$3^4 \cdot 5^2$
	$PSL(3,4) : 2$	$3^4 \cdot 5^2 \cdot 11$
	$2 \cdot A_8$	$3^4 \cdot 5^2 \cdot 11$
	$2^4 : A_7$	$3^4 \cdot 5^2 \cdot 11$
McL $\cdot$ 2	$U_4(3) : 2$	$5^2 \cdot 11$
	$PSL(3,4) : 2^2$	$3^4 \cdot 5^2 \cdot 11$
	$2 \cdot S_8$	$3^4 \cdot 5^2 \cdot 11$
	$2^{2+4} : (S_3 \times S_3)$	$3^4 \cdot 5^3 \cdot 7 \cdot 11$
HN	$2^{1+8} \cdot (A_5 \times A_5) \cdot 2$	$3^4 \cdot 5^4 \cdot 7 \cdot 11 \cdot 19$
	$2^3 \cdot 2^2 \cdot 2^6 \cdot (3 \times PSL(3,2))$	$3^4 \cdot 5^6 \cdot 11 \cdot 19$
HN $\cdot$ 2	$2^{1+8} \cdot (A_5 \times A_5) \cdot 2^2$	$3^4 \cdot 5^4 \cdot 7 \cdot 11 \cdot 19$
	$2^3 \cdot 2^2 \cdot 2^6 \cdot (3 \times PSL(3,2)) \cdot 2$	$3^4 \cdot 5^6 \cdot 11 \cdot 19$
BM	$2^{1+22} \cdot \mathrm{Co}_2$	$3^7 \cdot 5^3 \cdot 7 \cdot 13 \cdot 19 \cdot 31 \cdot 47$
	$2^{9+16} \cdot S_8(2)$	$3^8 \cdot 5^4 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 23 \cdot 31 \cdot 47$

	$2^{2+10+20} : (M_{22:2\times S_3})$ $2^{3+(1\cdot 4)+1\cdot 2+(12\cdot 3)} \cdot (S_5 \times PSL(3,2))$	$3^{10} \cdot 5^5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$ $3^{11} \cdot 5^5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$
M	$2^{1+24} \cdot \mathrm{Co}_1$	$3^{11} \cdot 5^5 \cdot 7^4 \cdot 11 \cdot 13^2 \cdot 17 \cdot 19 \cdot 29$ $\cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$
	$2^{10+16} \cdot O_{10}^{+}(2)$	$3^{15} \cdot 5^7 \cdot 7^5 \cdot 11^2 \cdot 13^2 \cdot 13^3 \cdot 19 \cdot 23$ $\cdot 29 \cdot 41 \cdot 47 \cdot 59 \cdot 71$
	$2^{2+11+22} \cdot (M_{24} \times S_3)$	$3^{16} \cdot 5^8 \cdot 7^5 \cdot 11 \cdot 13^2 \cdot 17 \cdot 19 \cdot 29$ $\cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$
	$2^{5+10+20} \cdot (S_3 \times PSL(5,2))$	$3^{17} \cdot 5^8 \cdot 7^5 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23$ $\cdot 29 \cdot 41 \cdot 47 \cdot 59 \cdot 71$
	$2^{3+6+12+18}(PSL(3,2) \times 3S_6)$	$3^{17} \cdot 5^8 \cdot 7^5 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23$ $\cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$

Table 5.3: Odd useful indices and potential primes

X	m_X	p_X
M_{11}	11	11
M_{12}	$3^2 \cdot 5 \cdot 11$	$5, 11$
$M_{12} \cdot 2$	$3^2 \cdot 5 \cdot 11$	$5, 11$
M_{22}	$7 \cdot 11$	$7, 11$
$M_{22} \cdot 2$	$7 \cdot 11$	$7, 11$
M_{23}	23	23
M_{24}	$3 \cdot 11 \cdot 23$	$11, 23$
J_1	$5 \cdot 11 \cdot 19$	$5, 11, 19$
J_2	$3^2 \cdot 5 \cdot 7$	7
$J_2 \cdot 2$	$3^2 \cdot 5 \cdot 7$	7
J_3	$3^4 \cdot 17 \cdot 19$	$17, 19$
$J_3 \cdot 2$	$3^4 \cdot 17 \cdot 19$	$17, 19$
J_4	$11^2 \cdot 29 \cdot 31 \cdot 37 \cdot 43$	$29, 31, 37, 43$
HS	$3 \cdot 5^3 \cdot 11$	11
HS $\cdot 2$	$3 \cdot 5^3 \cdot 11$	11
Suz	$3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$7, 11, 13$
Suz $\cdot 2$	$3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$7, 11, 13$
McL	$5^2 \cdot 11$	11
McL $\cdot 2$	$5^2 \cdot 11$	11
Ru	$3^2 \cdot 5^3 \cdot 13 \cdot 29$	$13, 29$
He	$5 \cdot 7^3 \cdot 17$	17
He $\cdot 2$	$3^2 \cdot 5^2 \cdot 7^2 \cdot 17$	17
Ly	$5^3 \cdot 31 \cdot 37 \cdot 67$	$31, 37, 67$
O'N	$3^2 \cdot 7^2 \cdot 11 \cdot 19 \cdot 31$	$11, 19, 31$

$\mathrm{O'N} \cdot 2$	$3^2 \cdot 7^2 \cdot 11 \cdot 19 \cdot 31$	$11, 19, 31$
Co_1	$3^6 \cdot 5^3 \cdot 7 \cdot 13$	13
Co_2	$3^4 \cdot 5^2 \cdot 23$	23
Co_3	$3^3 \cdot 5^2 \cdot 11 \cdot 23$	$11, 23$
Fi_{22}	$3^7 \cdot 5 \cdot 13$	13
$\mathrm{Fi}_{22} \cdot 2$	$3^7 \cdot 5 \cdot 13$	13
Fi_{23}	$3^4 \cdot 17 \cdot 23$	$17, 23$
Fi_{24}'	$3^{13} \cdot 5 \cdot 7^2 \cdot 13 \cdot 17 \cdot 29$	$11, 13, 17, 23, 29$
$\mathrm{Fi}_{24}' \cdot 2$	$3^{13} \cdot 5 \cdot 7^2 \cdot 13 \cdot 17 \cdot 29$	$11, 13, 17, 23, 29$
HN	$3^4 \cdot 5^4 \cdot 7 \cdot 11 \cdot 19$	$7, 11, 19$
$\mathrm{HN} \cdot 2$	$3^4 \cdot 5^4 \cdot 7 \cdot 11 \cdot 19$	$7, 11, 19$
Th	$3^8 \cdot 5^2 \cdot 7 \cdot 13 \cdot 19$	$13, 19$
BM	$3^7 \cdot 5^3 \cdot 7 \cdot 13 \cdot 19 \cdot 31 \cdot 47$	$13, 19, 31, 47$
M	$3^{11} \cdot 5^5 \cdot 7^4 \cdot 11 \cdot 13^2 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$	$17, 19, 29, 31, 41, 47, 59, 71$

Table 5.4: n_X

X	$n(X)$
Co_1	$3^4 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 23$
Fi_{22}	$3^5 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
Fi_{24}'	$3^9 \cdot 5 \cdot 11 \cdot 7^2 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
$\mathrm{Aut}(\mathrm{Fi}_{24}')$	$3^9 \cdot 5 \cdot 11 \cdot 7^2 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
Th	$3^8 \cdot 5^2 \cdot 7 \cdot 13 \cdot 19 \cdot 31$

Chapter 6

Miscellaneous

From Theorem 1.2.2, Theorem 1.2.6, Theorem A and Theorem C, we obtain the following.

Theorem 6.0.2. *Let G be a finitely generated profinite group and S a finite simple group. Assume that almost every composition factor of G is isomorphic to S. Then $P_G(s)$ is rational if and only if $G/\mathrm{Frat}(G)$ is a finite group.*

We would like to ask whether the conjecture holds if we replace the simple group S in Theorem 6.0.2 by a finite set $\mathcal{F}$ of simple groups. The problem is not easy even in the case $\mathcal{F}$ is of cardinality 2. In the first section, we give some examples showing difficulties for this situation. However, there are some cases in which the conjecture holds, as can be seen in the second section.

6.1 Examples

In this section, we will give some examples showing that our techniques are not effective in the general case.

Example 1 In this example, we consider the group G such that almost every composition factor of G is either an alternating group $\mathrm{Alt}(m)$ or isomorphic to a projective special linear group $\mathrm{PSL}(n, p)$. We will show that we cannot deduce the finiteness of $\pi(G)$ by our techniques.

Assume that $P_G(s)$ is factorized as

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

where J is the set of indices i such that the chief factor G_i/G_{i+1} is non-Frattini and Γ the set of the simple groups S_i with $i \in J$. Let I be the set of indices $i \in J$ such that S_i is either an alternating group or a projective special linear group, and let Γ^* be the set of simple groups such that $S_i \in \Gamma$ with $i \in I$. By our assumption, the Dirichlet series $A(s) = \prod_{i \in I} P_i(s)$ is rational, and hence $\pi(A(s))$ is finite. Assume that $p = 5$ does not belong to $\pi(A(s))$, as in Step 1 in Section 2.6.1. We need to prove that 5 is actually in $\pi(A(s))$ to obtain a contradiction. Let

$$\mathcal{S} = \{S \in \Gamma^* : 5 \in \pi(P_i(s))\},\ r := \min\{r_i : S_i \in \mathcal{S}\} \text{ and } I^* := \{i \in I : r_i = r \text{ and } S_i \in \mathcal{S}\}$$

As in our process described in Section 2.6, we consider Λ the set of positive integers divisible by 5, and let $\beta \in \Lambda$ be minimal with the properties that $v_5(\beta) = r$ and $b_{i,\beta} \neq 0$ for some $i \in I$, i.e., β is a useful index for a group L_i with $i \in I$. At this step, we need to show that $b_{i,\beta} < 0$ for all i such that $b_{i,\beta} \neq 0$. However, if $S_i \cong \mathrm{Alt}(3.5.11)$ then

$$P_i(s) = 1 - \frac{3.5.11}{(3.5.11)^{r_i s}} + \cdots$$

while if $S_j \cong \mathrm{PSL}(2,11)$ then

$$P_j(s) = 1 - \frac{22}{11^{r_j s}} + \frac{165}{(3.5.11)^{r_j s}} + \cdots$$

In this case, $\beta = 3.5.11$, but $b_{i,\beta} < 0$ while $b_{j,\beta} > 0$. Thus, we can not conclude that

$$c_\beta = \sum_{\substack{i \in I^* \\ r_i = r}} b_{i,\beta}$$

is different from 0. Therefore, we cannot conclude that 5 is in fact in $\pi(A(s))$, eventhough $5 \in \pi(G)$. Hence, we cannot conclude that $\pi(G)$ is a finite set.

Example 2 In this example, we consider the group G in which both $\mathrm{PSL}(3,3)$ and $\mathrm{PSL}(12,2)$ appear infinitely many times as composition factors in non-Frattini chief factors of G. We will show that when the characteristics of simple groups of Lie type are different, then our techniques are not effective.

Assume in addition that $\pi(G)$ is finite. We need to prove the final step to deduce the finiteness of $G/\mathrm{Frat}(G)$. As above, the product

$$A(s) = \prod_{i \in I} P_i(s)$$

is rational. We would like to deduce the emptiness of the set I. We will use reduction maps in Lemma 1.2.5 to simplify the product $A(s)$. We choose the prime $p = 2$ and so the product

$$\prod_{i \in I} P_i^{(2)}(s)$$

is still rational. At this step, normally we will look for a positive integer w with some additional properties, such that we can use Proposition 2.4.3 to obtain that the following product

$$\prod_{i \in I} \left(1 + \frac{b_{i,w^{r_i}}}{(w^{r_i})^s}\right), \text{ where } b_{i,w^{r_i}} < 0$$

is still rational. From that, we can then use the Corollary of the Skolem-Mahler-Lech Theorem. However, if $S_i \cong \mathrm{PSL}(3,3)$ then

$$P_i^{(2)}(s) = 1 - \frac{26}{13^{r_i s}} + \frac{117}{(3^2.13)^{r_i s}}$$

while if $S_i \cong \mathrm{PSL}(12,2)$ then

$$P_i^{(2)}(s) = 1 - \frac{3^2.5.7.13}{(3^2.5.7.13)^{r_i s}} + \cdots .$$

In this situation, if we choose w in the set Λ of odd positive integers divisible by 3^2 and 13 such that $v_3(w) = 2$ and $v_{13}(w) = 1$, then if w would be $3^2.13$. So $b_{i,w^{r_i}} = 117 > 0$. Thus, if we could reduce $A(s)$ to the product

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

we still can't apply the Skolem-Mahler-Lech Theorem since not all $b_{i,w^{r_i}}$ are negative.

6.2 Mixing up some families of simple groups

In this section, we will give a proof of the following theorem.

Theorem D. *Let G be a finitely generated profinite group of which almost every composition factor is isomorphic to either a sporadic group, or a projective special linear group $PSL(2,p)$ for some prime $p \geq 5$, or an alternating group $Alt(n)$ where n is either a prime or a power of 2. If $P_G(s)$ is rational then $G/\mathrm{Frat}(G)$ is a finite group.*

We will use the techniques as in Chapter 4 and Chapter 5. We will focus on the smallest useful index in the monolithic group associated to a nonabelian composition factor $S \in \Gamma^*$. Descriptions of such useful indices when S is $\mathrm{PSL}(2,p)$ or sporadic are included in Chapters 4 and 5. We now focus on the alternating groups $\mathrm{Alt}(n)$ when n is either a prime or a power of 2.

When $n = p$ is a prime number, $\mathrm{Alt}(p)$ has a maximal subgroup $M = \mathrm{Alt}(p-1)$ of index p, and similarly for $\mathrm{Sym}(p)$.

6.2.1 Maximal subgroups in alternating groups Alt(2^t)

Let X be an almost simple group whose socle is $\mathrm{Alt}(n)$ where $n = 2^t$ is a power of 2, with $t \geq 3$. So either $X = \mathrm{Alt}(n)$ or $X = \mathrm{Sym}(n)$.

Let M be a maximal subgroup of X such that M contains a Sylow 2-subgroup of X. By Liebeck and Saxl ([LS85]), the group M is of either intransitive type or imprimitive type unless $n = 8$ and $X = \mathrm{Alt}(8)$.

- In case M is of intransitive type, i.e., $M = (S_k \times S_{n-k}) \cap X$ with $1 \leq k < n/2$, then
$$|X : M| = \binom{n}{k}.$$
Let $n = \sum_i n_i 2^i$ and $k = \sum_i k_i 2^i$ be 2-adic expansions of n and k respectively, then applying Lucas' Theorem gives us
$$|X : M| = \binom{n}{k} \equiv \prod_i \binom{n_i}{k_i} \equiv 0 \mod 2$$
since $n_i = 0$ for all but $i = t$. Therefore M is always of even index in X, a contradiction. Hence M is not intransitive.

- In case M is of imprimitive type, i.e., $M = (S_a \wr S_b) \cap X$ where $ab = 2^t, a > 1, b > 1$, then M has index
$$w(a,b) = \frac{(2^t)!}{(a!)^b.b!}.$$
Notice that $w(a,b)$ is always odd because of the following. For a given integer n, let $n = a_0 + a_1 p + \cdots + a_d p^d$ be the p-adic expansion of n where p is a prime and $0 \leq a_j \leq p-1$ for each j, $a_d \neq 0$. Let $S_p(n) = a_0 + \cdots + a_d$, then Legendre's formula gives us
$$v_p(n!) = \frac{n - S_p(n)}{p-1}.$$
Now in this case $n = 2^t$, then $p = 2, a_t = 1$ and $a_k = 0$ for all $k \neq t$. So $S_2(n) = 1$. We have that $v_2(n!) = 2^t - 1$. Assume that $a = 2^u, b = 2^v$ then $v_2(a) = 2^u - 1$, $v_2(b) = 2^v - 1$ so that
$$v_2((2^u!)^{2^v}) = (2^u - 1)2^v.$$
Then
$$v_2((2^u!)^{2^v}.2^v!) = (2^u - 1)2^v + 2^v - 1 = 2^{u+v} - 1 = 2^t - 1.$$
Hence $w(a,b)$ is always odd.

- In case $n = 8$ and $X = \mathrm{Alt}(8)$ then $M = 2^3 : \mathrm{PSL}(3,2)$. So $|X : M| = 3 \cdot 5$.

Lemma 6.2.1. *[Mar02, Lemma 2.1] Assume that $m = ab \geq 8, a, b \geq 2$. Then*
$$w(a,b) = \frac{m!}{a!^b.b!}$$
is smallest when b is the smallest prime divisor of n.

Proof. We may assume that $a \geq b$ since if $b > a$ then
$$b!^{a-1} = a!^{a-1}(a+1)^{a-1} \cdots b^{a-1} > a!^{a-1}a^{(b-a)(a-1)}.$$
In addition, we have that $a^{a-1} > 1.2. \cdots .a = a!$ and so
$$b!^{a-1} > a!^{a-1}a!^{b-a} = a!^{b-1}$$
which implies that
$$b!^a.a! > a!^b.b! \Rightarrow \frac{m!}{a!^b.b!} > \frac{m!}{b!^a.a!}.$$

Assume now that $m = a_1 b_1 = a_2 b_2$ with $b_1 \leq a_1, b_2 \leq a_2$. If $b_1 \leq b_2$ then $a_1 \geq a_2$ and

$$\begin{aligned}
a_1!^{b_1}.b_1! &\geq a_2!^{b_1}(a_2+1)^{b_1}\cdots a_1^{b_1} b_1! \geq a_2!^{b_1} a_2^{(a_1-a_2)b_1} b_1! \quad (\text{since } a_1 \geq a_2) \\
&= a_2!^{b_1} b_1! (a_2^{a_2})^{\frac{b_1}{a_2}(a_1-a_2)} = a_2!^{b_1} b_1! (a_2^{a_2-1} a_2)^{\frac{b_1}{a_2}(a_1-a_2)} \\
&\geq a_2!^{b_1} b_1! (a_2! b_2)^{\frac{b_1}{a_2}(a_1-a_2)} = a_2!^{b_1} b_1! (a_2! b_2)^{b_2-b_1} \quad (\text{since } a_2 \geq b_2 \text{ and } a_1 b_1 = a_2 b_2) \\
&\geq a_2!^{b_2} b_1! (b_1+1)\cdots b_2 = a_2!^{b_2} b_2! \quad (\text{since } b_2 \geq b_1)
\end{aligned}$$

and hence

$$\frac{m!}{a_1!^{b_1}.b_1!} \leq \frac{m!}{a_2!^{b_2}.b_2!}$$

□

In particular, when $n = 2^t$, then $w(2^{t-1}, 2)$ is the smallest among $w(a, b)$ with $n = ab$, $a > 1, b > 1$.

Theorem 6.2.2. *Let L be a monolithic primitive group with socle is $(Alt(2^t))^r$. Let*

$$w = \begin{cases} (2^t)!/((2^{t-1}!)^2 \cdot 2!) & \text{if } t > 3, \\ 3 \cdot 5 & \text{if } t = 3. \end{cases}$$

Let q be the largest prime less than 2^t if $t > 3$ and $q = 5$ otherwise. Then w^r is the smallest odd q-useful index for L.

6.2.2 The main result

Let G now be a finitely generated profinite group of which almost every nonabelian composition factor is isomorphic to either a sporadic group, or a projective special linear group $\mathrm{PSL}(2, p)$ for some prime $p \geq 5$, or an alternating group $\mathrm{Alt}(n)$ where n is either a prime or a power of 2. Assume in addition that $P_G(s)$ is rational.

We fix a descending normal series $\{G_i\}$ of G with the properties that $\bigcap G_i = 1$ and G_i/G_{i+1} is a chief factor of G/G_{i+1}. Let J be the set of indices i with G_i/G_{i+1} non-Frattini. Then by Section 2.1, the probabilistic zeta function $P_G(s)$ can be factorized as

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

where for each i, the finite Dirichlet series $P_i(s)$ is associated to the chief factor G_i/G_{i+1}. We have the following crucial result.

Proposition 6.2.3. *The set $\pi(G)$ is finite.*

Proof. Let Γ be the set of simple groups that appear as composition factors in non-Frattini chief factors of G. Let Γ^* be the subset of Γ containing simple groups $S_i \in \Gamma$ such that S_i is isomorphic to either a sporadic simple group, or $\mathrm{PSL}(2,p)$ for some prime $p \geq 5$, or an alternating group $\mathrm{Alt}(n)$ where n is either a prime or a power of 2.

Notice that for each simple group $S \in \Gamma^*$ which is not sporadic, either there is an odd prime r such that $S \cong \mathrm{PSL}(2,r)$ or $S \cong \mathrm{Alt}(r)$ or $S \cong \mathrm{Alt}(2^t)$ for some $t \geq 3$. In the latter case, there is also an associated prime p_t, namely the largest prime less than 2^t. Notice also that for a given prime p, there are only finitely many numbers n such that p is the largest prime less than n, since for every large enough positive integer x, there is always a prime in the interval $[x, 6/5x]$ (see [Nag52]). Now we proceed as in Chapter 4 and 5.

Assume by contradiction that Γ^* is infinite. Let I be the set of indices i such that $S_i \in \Gamma^*$ and let $A(s) = \prod_{i \in I} P_i(s)$, $B(s) = \prod_{i \in J \setminus I} P_i(s)$. Since $\pi(P_G(s))$ is finite and by hypothesis, $\pi(B(s))$ is finite, it follows that $\pi(A(s))$ is finite. In particular, there is a prime $p > 71$ such that $p \notin \pi(A(s))$. We choose the prime number $p > 71$ since 71 is the largest prime dividing the order of a sporadic simple group, so if p divides some $|S_i|$ then S_i is either an alternating group or a projective special linear group. Set

$$I^* = \{i \in I : p \in \pi(P_i(s))\} \quad \text{and} \quad r = \min\{r_i : i \in I^*\}.$$

Let Λ be the set of all odd positive integers n such that n is divisible by p and is not divisible by any prime strictly larger than p. Notice that for each $i \in I^*$, there exists $\alpha \in \Lambda$ such that α is a useful index for L_i. Indeed, if $p \in \pi(P_i(s))$ then one of the following occurs:

- $S_i = \mathrm{PSL}(2,p)$ and $(p(p \pm 1)/2)^{r_i}$ are useful indices for L_i.

- $S_i = \mathrm{Alt}(p)$ and p^{r_i} is a useful index for L_i.

- $S_i = \mathrm{Alt}(2^t)$ and $w(2^t, 2)$ is a useful index for L_i.

Choose $\alpha \in \Lambda$ minimal with the properties that there exists $i \in I^*$ such that $r_i = r$, and $v_p(\alpha) = r$ and α is a useful index for L_i. Notice that if $i \in I$ such that $b_{i,\alpha} \neq 0$ then $i \in I^*$, and $r_i = r$ and α is the smallest odd p-useful index for L_i. It follows that $b_{i,\alpha} < 0$. Hence the coefficient c_α of $1/\alpha^s$ in $A(s)$ is

$$c_\alpha = \sum_{\substack{i \in I \\ r = r_i}} b_{i,\alpha} = \sum_{i \in I^*} b_{i,\alpha} < 0$$

which implies that $p \in \pi(A(s))$, a contradiction. Hence Γ^*. It follows that Γ is finite. Consequently, the set $\pi(G)$ is also finite. □

Proof of Theorem D. Let $\mathcal{T}$ be the set of almost simple groups X such that there are infinitely many indices $i \in J$ with $X_i \cong X$, and let $I = \{i \in J : X_i \cong X\}$. Our assumptions combined with Proposition 2.6.3, imply that $J \setminus I$ is finite. In order to prove that J is finite, we need to prove that I is empty. Since $P_G(s)$ is rational, also $\prod_{i \in I} P_i(s)$ is rational. By Lemma 1.2.5, the product $\prod_{i \in I} P_i^{(2)}(s)$ is still rational. Notice that the set $\pi(\mathcal{T})$ of prime divisors of orders of simple groups S such that $S = \mathrm{soc}(X)$ for some $X \in \mathcal{T}$ is finite. Let

$$q = \max\{p : p \in \pi(\mathcal{T})\}$$

and

$$\Lambda_q = \{i \in I : q \in \pi(P_i^{(2)}(s))\}.$$

Notice that if $q > 71$ and $i \in \Lambda_q$ then S_i is isomorphic to either $\mathrm{Alt}(q)$ or $\mathrm{Alt}(2^t)$, where q is the largest prime less than 2^t, or $\mathrm{PSL}(2, q)$. Let

$$\begin{aligned} w &= \min\{x \in \mathbb{N} \mid x \text{ is odd}, v_q(x) = 1 \text{ and } b_{i,x^{r_i}} \neq 0 \text{ for some } i\} \\ &= \min\{x \in \mathbb{N} \mid x \text{ is odd}, v_q(x) = 1 \text{ and } b_{i,x^{r_i}} \neq 0 \text{ for some } i \in \Lambda_q\}. \end{aligned}$$

Note that if $i \in \Lambda_q$, and n is minimal with the properties that n is odd, $b_{i,n^{r_i}} \neq 0$ and $v_q(n) = 1$, then $b_{i,n^{r_i}} < 0$. So if $b_{i,n^{r_i}} \neq 0$ then $b_{i,n^{r_i}} < 0$. Moreover, by Proposition 2.4.3, we obtain the rational product

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

where $b_{i,w^{r_i}} \leq 0$ for each $i \in \Lambda_q$. By applying Corollary 2.5.5, we get that $\Lambda_q^* = \{i \in \Lambda_q \mid b_{i,w^{r_i}} \neq 0\}$ is finite, but this implies that $\Lambda_q = \emptyset$. Let

$$p = \max\{r : r \in \pi(\mathcal{T}) \setminus \{q\}\}$$

and

$$\Lambda_p = \{i \in I : p \in \pi(P_i^{(2)}(s))\}.$$

Again, by the same argument, we obtain that $\Lambda_p = \emptyset$. We continue this procedure until we reach the prime 71. Notice that we deal with both $\mathrm{PSL}(2,71), \mathrm{Alt}(71)$ and M by the prime 71. Now, with the same spirit, we deal with all remaining sporadic groups, alternating groups and $\mathrm{PSL}(2,q)$ with $5 \leq q < 71$. Our process is described in order in the following table in which the first column stands for the primes r we use in order to deduce that $\Lambda_r = \emptyset$, the second column are simple groups S involved corresponding to the primes in the first column:

r	S
71	$\mathrm{PSL}(2,71), \mathrm{M}, \mathrm{Alt}(71)$
67	$\mathrm{PSL}(2,67), \mathrm{Alt}(67), \mathrm{Ly}$
61	$\mathrm{Alt}(61), \mathrm{Alt}(2^6)$
59	$\mathrm{PSL}(2,59), \mathrm{Alt}(59)$
53	$\mathrm{PSL}(2,53), \mathrm{Alt}(53)$
47	$\mathrm{PSL}(2,47), \mathrm{Alt}(47), \mathrm{BM}$
43	$\mathrm{PSL}(2,43), \mathrm{Alt}(43), J_4$
41	$\mathrm{PSL}(2,41), \mathrm{Alt}(41)$
37	$\mathrm{PSL}(2,37), \mathrm{Alt}(37)$
31	$\mathrm{PSL}(2,31), \mathrm{Alt}(31), \mathrm{Alt}(2^5), \mathrm{O'N}$
29	$\mathrm{PSL}(2,29), \mathrm{Alt}(29), \mathrm{Fi'}_{24}, \mathrm{Ru}$
23	$\mathrm{PSL}(2,23), \mathrm{Alt}(23), \mathrm{M}_{23}, \mathrm{M}_{24}, \mathrm{Co}_2, \mathrm{Co}_3, \mathrm{Fi}_{23}$
19	$\mathrm{PSL}(2,19), \mathrm{Alt}(19), J_1, J_3, \mathrm{HN}, \mathrm{Th}$
17	$\mathrm{PSL}(2,17), \mathrm{Alt}(17), \mathrm{He}$
13	$\mathrm{PSL}(2,13), \mathrm{Alt}(13), \mathrm{Alt}(2^4), \mathrm{Suz}, \mathrm{Co}_1, \mathrm{Fi}_{22}$
11	$\mathrm{PSL}(2,11), \mathrm{Alt}(11), M_{11}, M_{12}, M_{22}, \mathrm{HS}, \mathrm{McL}$
7	$\mathrm{PSL}(2,7), \mathrm{Alt}(7), J_2$
5	$\mathrm{PSL}(2,5), \mathrm{Alt}(5), \mathrm{Alt}(2^3)$

□

6.2.3 Appendix

Table 6.2: Even numbers n with largest prime less than 71 and potential primes p such that $v_p(w) = 1$ where $w = n!/(m!)^t.t!$

n	potential primes
10	7
12	7, 11
14	11, 13
16	11, 13
18	11, 13, 17
20	11, 13, 17, 19
22	13, 17, 19
24	13, 17, 19, 23
26	17, 19, 23
28	17, 19, 23
30	17, 19, 23, 29
32	17, 19, 23, 29, 31
34	19, 23, 29, 31
36	19, 23, 29, 31
38	23, 29, 31, 37
40	23, 29, 31, 37
42	23, 29, 31, 37, 41
44	23, 29, 31, 37, 41, 43
46	29, 31, 37, 41, 43
48	29, 31, 37, 41, 43, 47
50	29, 31, 37, 41, 43, 47
52	29, 31, 37, 41, 43, 47
54	29, 31, 37, 41, 43, 47, 53
56	29, 31, 37, 41, 43, 47, 53
58	31, 37, 41, 43, 47, 53
60	31, 37, 41, 43, 47, 53, 59
62	37, 41, 43, 47, 53, 59, 61
64	37, 41, 43, 47, 53, 59, 61
66	37, 41, 43, 47, 53, 59, 61
68	37, 41, 43, 47, 53, 59, 61, 67
70	37, 41, 43, 47, 53, 59, 61, 67
72	37, 41, 43, 47, 53, 59, 61, 67, 71

Table 6.3: Prime divisors of $|\mathrm{PSL}(2, q)|$ for $q \leq 71$

q	$\lvert\mathrm{PSL}(2, q)\rvert$	Smallest odd useful index
71	$2^3 \cdot 3^2 \cdot 7 \cdot 71$	$5 \cdot 7 \cdot 71$
67	$2^2 \cdot 3 \cdot 11 \cdot 17 \cdot 67$	$3 \cdot 11 \cdot 67$
61	$2^2 \cdot 3 \cdot 5 \cdot 31 \cdot 61$	$31 \cdot 61$

59	$2^2 \cdot 3 \cdot 5 \cdot 29 \cdot 59$	$29 \cdot 59$
53	$2^2 \cdot 3^2 \cdot 13 \cdot 53$	$3^3 \cdot 53$
47	$2^4 \cdot 3 \cdot 23 \cdot 47$	$23 \cdot 47$
43	$2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 43$	$3 \cdot 7 \cdot 43$
41	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 41$	$3 \cdot 7 \cdot 41$
37	$2^2 \cdot 3^2 \cdot 19 \cdot 37$	$19 \cdot 37$
31	$2^5 \cdot 3 \cdot 5 \cdot 31$	$3 \cdot 5 \cdot 31$
29	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 29$	$29 \cdot 7$
23	$2^3 \cdot 3 \cdot 11 \cdot 23$	$11 \cdot 23$
19	$2^2 \cdot 3^2 \cdot 5 \cdot 19$	$19 \cdot 3$
17	$2^4 \cdot 3^2 \cdot 17$	$3^2 \cdot 17$
13	$2^2 \cdot 3 \cdot 7 \cdot 13$	$7 \cdot 13$
11	$2^2 \cdot 3 \cdot 5 \cdot 11$	11
7	$2^3 \cdot 3 \cdot 7$	7
5	$2^2 \cdot 3 \cdot 5$	5

Bibliography

[Asc00] M. Aschbacher. *Finite group theory*, volume 10 of *Cambridge Studies in Advanced Mathematics*. Cambridge Univ. Press, 2000.

[BBE06] Adolfo Ballester-Bolinches and Luis M. Ezquerro. *Classes of finite groups*, volume 584 of *Mathematics and Its Applications (Springer)*. Springer, Dordrecht, 2006.

[Bos96] Nigel Boston. A probabilistic generalization of the riemann zeta function. In *Analytic Number Theory*, volume 1, pages 155–162, 1996.

[Bou00] Serge Bouc. Polynomial ideals and classes of finite groups. *J. Algebra*, 229(1):153–174, 2000.

[BPS96] Alexandre V. Borovik, Laszlo Pyber, and Aner Shalev. Maximal subgroups in finite and profinite groups. *Trans. Amer. Math. Soc.*, 348(9):3745–3761, 1996.

[Bro00] K. S. Brown. The coset poset and probabilistic zeta function of a finite group. *J. Algebra*, 225:989–1012, 2000.

[Car72] R. W. Carter. *Simple groups of Lie type*. John Wiley & Sons, 1972.

[CL10] Valentina Colombo and Andrea Lucchini. On subgroups with non-zero Möbius numbers in the alternating and symmetric groups. *J. Algebra*, 324(9):2464–2474, 2010.

[DdSMS99] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p groups*, volume 61 of *Cambridge Studies in Advanced Mathematics*. Cambridge Univ. Press, second edition, 1999.

[Dic58] Leonard Eugene Dickson. *Linear groups: With an exposition of the Galois field theory*. with an introduction by W. Magnus. Dover Publications Inc., New York, 1958.

[Dix69] John D. Dixon. The probability of generating the symmetric group. *Math. Z.*, 110:199–205, 1969.

[Dix02] John D. Dixon. Probabilistic group theory. *C. R. Math. Acad. Sci. Soc. R. Can.*, 24(1):1–15, 2002.

[DL02] Erika Damian and Andrea Lucchini. The dirichlet polynomial of a finite group and the subgroups of prime power index. *Advances in group theory*, pages 209–221, 2002.

[DL03a] Eloisa Detomi and Andrea Lucchini. Crowns and factorization of the probabilistic zeta function of a finite group. *J. Algebra*, 265(2):651–668, 2003.

[DL03b] Eloisa Detomi and Andrea Lucchini. Recognizing soluble groups from their probabilistic zeta functions. *Bull. London Math. Soc.*, 35(5):659–664, 2003.

[DL04a] E. Damian and A. Lucchini. Recognizing the alternating groups from their probabilistic zeta function. *Glasg. Math. J.*, 46(3):595–599, 2004.

[DL04b] Eloisa Detomi and Andrea Lucchini. Profinite groups with multiplicative probabilistic zeta function. *J. London Math. Soc.*, 70(2):165–181, 2004.

[DL05] Erika Damian and Andrea Lucchini. A probabilistic generalization of subnormality. *J. Algebra Appl.*, 4(3):313–323, 2005.

[DL06a] Erika Damian and Andrea Lucchini. On the dirichlet polynomial of finite groups of lie type. *Rendiconti del Seminario Matematico della Universita di Padova*, 115:51–69, 2006.

[DL06b] Eloisa Detomi and Andrea Lucchini. Crowns in profinite groups and applications. In *Noncommutative algebra and geometry*, volume 243 of *Lect. Notes Pure Appl. Math.*, pages 47–62. Chapman & Hall, 2006.

[DL06c] Eloisa Detomi and Andrea Lucchini. Profinite groups with a rational probabilistic zeta function. *Journal of Group Theory*, 9(2):203–217, 2006.

[DL07a] Erika Damian and Andrea Lucchini. Finite groups with p-multiplicative probabilistic zeta function. *Communications in Algebra*, 35:3451–3472, 2007.

[DL07b] Eloisa Detomi and Andrea Lucchini. Non-prosoluble profinite groups with a rational probabilistic zeta function. *Journal of Group Theory*, 10(4):453–466, 2007.

[DLM04] Erika Damian, Andrea Lucchini, and Fiorenza Morini. Some properties of the probabilistic zeta function on finite simple groups. *Pacific J. Math.*, 215(1):3–14, 2004.

[ET65] P. Erdős and P. Turán. On some problems of a statistical group-theory. I. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, 4:175–186 (1965), 1965.

[ET67a] P. Erdős and P. Turán. On some problems of a statistical group-theory. II. *Acta math. Acad. Sci. Hungar.*, 18:151–163, 1967.

[ET67b] P. Erdős and P. Turán. On some problems of a statistical group-theory. III. *Acta Math. Acad. Sci. Hungar.*, 18:309–320, 1967.

[ET68] P. Erdős and P. Turán. On some problems of a statistical group-theory. IV. *Acta Math. Acad. Sci. Hungar*, 19:413–435, 1968.

[ET70] P. Erdős and P. Turán. On some problems of a statistical group theory. VI. *J. Indian Math. Soc.*, 34(3-4):175–192 (1971), 1970.

[ET71] P. Erdős and P. Turán. On some problems of a statistical group theory. V. *Period. Math. Hungar.*, 1(1):5–13, 1971.

[ET72] P. Erdős and P. Turán. On some problems of a statistical group theory. VII. *Period. Math. Hungar.*, 2:149–163, 1972. Collection of articles dedicated to the memory of Alfréd Rényi, I.

[FJ08] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.

[Gas59] Wolfgang Gaschütz. Die Eulersche Funktion endlicher auflösbarer Gruppen. *Illinois J. Math.*, 3:469–476, 1959.

[Gur83] Robert M. Guralnick. Subgroups of prime power index in a simple group. *Journal of Algebra*, 81(2):304–311, 1983.

[Hal36] P. Hall. The eulerian functions of a group. *Quart. J. Math.*, 7(1):134–151, 1936.

[Hal50] Marshall Hall. A topology for free groups and related groups. *Annals of Mathematics*, 52(1):127–139, 1950.

[JZP11] Andrei Jaikin-Zapirain and László Pyber. Random generation of finite and profinite groups and group enumeration. *Ann. of Math. (2)*, 173(2):769–814, 2011.

[KL90a] W.M. Kantor and A. Lubotzky. The probability of generating a finite classical group. *Geom. Ded.*, 36:67–87, 1990.

[KL90b] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*, volume 243 of *Lect. Notes Pure Appl. Math.* Cambridge Univ. Press, 1990.

[LPS88] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl. On the O'Nan-Scott theorem for finite primitive permutation groups. *J. Austral. Math. Soc. Ser. A*, 44(3):389–396, 1988.

[LS85] Martin W. Liebeck and Jan Saxl. The primitive permutation groups of odd degree. *J. London Math. Soc. (2)*, 31(2):250–264, 1985.

[LS95] Martin W. Liebeck and Aner Shalev. The probability of generating a finite simple group. *Geom. Dedicata*, 56(1):103–113, 1995.

[LS03] Alexander Lubotzky and Dan Segal. *Subgroup growth*, volume 212 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 2003.

[Luc07] Andrea Lucchini. Subgroups of solvable groups with non-zero Möbius function. *J. Group Theory*, 10(5):633–639, 2007.

[Luc10] Andrea Lucchini. On the subgroups with non-trivial Möbius number. *J. Group Theory*, 13(4):589–600, 2010.

[Luc11a] Andrea Lucchini. On profinite groups with polynomially bounded Möbius numbers. *J. Group Theory*, 14(2):261–271, 2011.

[Luc11b] Andrea Lucchini. Profinite groups with nonabelian crowns of bounded rank and their probabilistic zeta function. *Israel J. Math.*, 181:53–64, 2011.

[Man96] A. Mann. Positively finitely generated groups. 1996.

[Man04] Avinoam Mann. Some applications of probability in group theory. In *Groups: topological, combinatorial and arithmetic aspects*, volume 311 of *London Math. Soc. Lecture Note Ser.*, pages 318–326. Cambridge Univ. Press, 2004.

[Man05] Avinoam Mann. A probabilistic zeta function for arithmetic groups. *Internat. J. Algebra Comput.*, 15(5-6):1053–1059, 2005.

[Mar02] Attila Maróti. On the orders of primitive groups. *J. Algebra*, 258:631–640, 2002.

[MS96] Avinoam Mann and Aner Shalev. Simple groups, maximal subgroups, and probabilistic aspects of profinite groups. *Israel J. Math.*, 96(part B):449–468, 1996.

[Nag52] Jitsuro Nagura. On the interval containing at least one prime number. *Proc. Japan Acad.*, 28:177–181, 1952.

[NS07] Nikolay Nikolov and Dan Segal. On finitely generated profinite groups. I. Strong completeness and uniform bounds. *Ann. of Math. (2)*, 165(1):171–238, 2007.

[Pat] Massimiliano Patassini. On the irreducibility of the Dirichlet polynomial of an alternating group. *Trans. Amer. Math. Soc.*, to appear.

[Pat09] Massimiliano Patassini. The probabilistic zeta function of $PSL(2,q)$, of the Suzuki groups ${}^2B_2(q)$ and of the Ree groups ${}^2G_2(q)$. *Pacific J. Math.*, 240(1):185–200, 2009.

[Pat11a] Massimiliano Patassini. On the dirichlet polynomial of the simple groups of lie type. Phd thesis, Universita di Padova, 2011.

[Pat11b] Massimiliano Patassini. On the irreducibility of the Dirichlet polynomial of a simple group of Lie type. *Israel J. Math.*, 185:477–507, 2011.

[Pat11c] Massimiliano Patassini. On the (non-)contractibility of the order complex of the coset poset of a classical group. *J. Algebra*, 343:37–77, 2011.

[RZ10] Luis Ribes and Pavel Zalesskii. *Profinite groups*, volume 40 of *A series of Modern Surveys in Mathematics*. Springer, second edition, 2010.

[Ser08] P. Jimnez Seral. Coefficient of the probabilistic zeta function of a monolithic group. *Galsgow J. Math*, 50:75–81, 2008.

[Sha98a] Aner Shalev. Simple groups, permutation groups, and probability. In *Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998)*, number Extra Vol. II, pages 129–137 (electronic), 1998.

[Sha98b] John Shareshian. On the probabilistic zeta function for finite groups. *J. Algebra*, 210(2):703–707, 1998.

[Sha01] Aner Shalev. Asymptotic group theory. *Notices Amer. Math. Soc.*, 48(4):383–389, 2001.

[Sta97] R. P. Stanley. *Enumerative combinatorics 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge Univ. Press, 1997.

[vdP89] A. J. van der Poorten. Some facts that should be better known, especially about rational functions. In *Number theory and applications (Banff, AB, 1988)*, volume 265 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 497–528. Kluwer Acad. Publ., Dordrecht, 1989.

[Wil98] John S. Wilson. *Profinite groups*, volume 19 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, New York, 1998.

[Zsi92] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3(1):265–284, 1892.

Samenvatting

In dit proefschrift onderzoeken we de relatie tussen eindig voortgebrachte pro-eindige groepen G en hun bijbehorende Dirichletreeks $P_G(s)$, waarvan de reciproke de probabilistische zètafunctie van G heet. In het bijzonder kijken we naar het vermoeden van Lucchini, dat zegt dat voor een eindig voortgebrachte pro-eindige groep G de bijbehorende Dirichletreeks $P_G(s)$ rationaal is dan en slechts dan als de quotiëntgroep $G/\mathrm{Frat}(G)$ eindig is. Detomi en Lucchini lieten al zien dat het vermoeden waar is voor pro-oplosbare G. Voor niet pro-oplosbare groepen hebben ze laten zien dat het vermoeden ook waar is als bijna elke niet-abelse compositiefactor van G een alternerende groep is. In dit proefschrift bevestigen we het vermoeden in een aantal andere gevallen. We laten eerst zien dat het vermoeden waar is als bijna elke niet-abelse compositiefactor van G isomorf is met een simpele groep van Lie-type over een lichaam van karakteristiek p, waar p een vaste priem is. Als er verschillende karakteristieken optreden, wordt het probleem moeilijker, en in dit geval hebben we nog geen antwoord. We verkrijgen wel als deelresultaat dat het vermoeden waar is als bijna elke niet-abelse compositiefactor van G isomorf is met één van de groepen $\mathrm{PSL}(2, p)$, met $p \geq 5$ priem. Dit is ook waar als we $\mathrm{PSL}(2, p)$ door een sporadische simpele groep vervangen. Het vermoeden staat in zijn algemeenheid nog open, en het kan door onze technieken niet bewezen worden. We geven een aantal voorbeelden die dit onderbouwen. Desondanks verkrijgen we in deze richting ook een gedeeltelijk resultaat door te laten zien dat het vermoeden waar is als bijna elke niet-abelse compositiefactor isomorf is met ofwel $\mathrm{PSL}(2, p)$, met $p \geq 5$ priem, of een sporadische simpele groep, of een alternerende groep $\mathrm{Alt}(n)$ waar n ofwel een priem, of een macht van 2 is.

Summary

In this thesis, we investigate the connection between finitely generated profinite groups G and the associated Dirichlet series $P_G(s)$ of which the reciprocal is called the probabilistic zeta function of G. In particular, we consider the conjecture of Lucchini saying that given a finitely generated profinite group G, the associated Dirichlet series $P_G(s)$ is rational if and only if the quotient group $G/\mathrm{Frat}(G)$ is finite. Detomi and Lucchini first showed that the conjecture holds when G is prosoluble. For non-prosoluble groups, they later showed that the conjecture also holds when almost every nonabelian composition factor of G is an alternating group. In this thesis, we prove the conjecture in several other cases. We first show that it holds when almost every nonabelian composition factor of G is isomorphic to a simple group of Lie type over a field of characteristic p, where p is a fixed prime. When there are different characteristics, the problem becomes quite difficult and we do not have any answer yet. However, we obtain that the conjecture holds when almost every nonabelian composition factor of G is $\mathrm{PSL}(2, p)$ for some prime $p \geq 5$. This is also the case when we replace $\mathrm{PSL}(2, p)$ by a sporadic simple group. The conjecture is still open in general and it cannot be proved by our techniques. We give some examples supporting this. Nevertheless, we also obtain a partial result by showing that the conjecture holds when almost every nonabelian composition factor is isomorphic to either $\mathrm{PSL}(2, p)$ for some prime $p \geq 5$, or a sporadic simple group, or an alternating group $\mathrm{Alt}(n)$ where n is either a prime or a power of 2.

Sommario

In questa tesi investighiamo la connessione tra un gruppo profinito finitamente generato G e la serie di Dirichlet associata $P_G(s)$, la cui inversa moltiplicativa è chiamata funzione zeta probabilistica di G. In particolare, consideriamo la congettura di Lucchini che dice che dato un gruppo profinito finitamente generato G, la serie di Dirichlet associata $P_G(s)$ è razionale se e solo se il quoziente $G/\mathrm{Frat}(G)$ è finito. Detomi e Lucchini hanno dimostrato la congettura nel caso prorisolubile. Per quanto riguarda i gruppi non prorisolubili, hanno dimostrato la congettura nell'ipotesi che quasi tutti i fattori non abeliani in una serie di composizione di G siano di tipo alterno. In questa tesi proviamo la congettura in alcuni altri casi non considerati in precedenza. La dimostriamo in particolare nell'ipotesi che quasi tutti i fattori di composizione non abeliani siano gruppi semplici di tipo Lie su campi di caratteristica p, con p un primo fissato. Quando la caratteristica varia il problema diventa piuttosto difficile e non abbiamo ancora risultati definitivi a riguardo. Tuttavia dimostriamo che la congettura vale se quasi ogni fattore di composizione non abeliano di G è della forma $\mathrm{PSL}(2, p)$ per qualche primo $p \geq 5$ (non fissato). Questo vale anche se sostituiamo $\mathrm{PSL}(2, p)$ con un gruppo semplice sporadico. La congettura è in generale ancora aperta e non può essere dimostrata con le tecniche utilizzate in questa tesi. Infatti sono forniti degli esempi in cui le nostre tecniche non producono risultati. Nonostante questo limite, abbiamo ottenuto un risultato parziale dimostrando che la congettura vale se quasi ogni fattore di composizione non abeliano è $\mathrm{PSL}(2, p)$ per qualche primo $p \geq 5$, oppure un gruppo semplice sporadico, oppure $\mathrm{Alt}(n)$ dove n è un primo o una potenza di 2.

Acknowledgements

First and foremost, I would like to present my deep sense of gratitude and reverence to my PhD supervisors, Prof. Andrea Lucchini and Prof. Hendrik W. Lenstra, for proposing to me an interesting Algant-Doc project, and for their enthusiasm, deep concern, able guidance and worthy counseling during its completion. I thank them for modeling the actions and behaviors of accomplished mathematicians and excellent teachers. I have learned so much from you through many conversations we have had, both in mathematics and others. They had profound influence on my professional and personal development by setting high standards on my work. Without them, I could not have finished my thesis. It has been much appreciated.

I gratefully acknowledge support from the Erasmus Mundus Program, whose ALGANT grant funded my master and PhD studies both in Padova and in Leiden. Many thanks to the professors in Padova and Leiden for their interesting and helpful courses, for their exciting discussions in mathematics, and for their help during my stay in Padova and Leiden.

I would like to send my big thanks to my family, specially to my wife, Uyen Nguyen, for their constant love and support. They are always the warmest and the most peaceful place for me in any case.

Last but not least, I would like to thank all my friends in Padova and Leiden for their support and help and for all the moments spent together during my master and PhD studies.

Curriculum Vitae

Duong Hoang Dung was born on September 13, 1985 in Dong Nai, Vietnam. After getting his bachelor from the Department of Mathematics in Ho Chi Minh city University of Pedagogy, he got a scholarship to follow the Algant-Master Erasmus Program. He spent his first year in the University of Padova, Italy, from October 2008 to June 2009, and his second year from September 2009 to June 2010 in Leiden University, the Netherlands. He did his master project with Jan Draisma from Eindhoven University of Technology on *Equivariant Gröbner Bases*. He then was awarded a fellowship to continue his PhD study in the Algant-Doc Joint Program between Leiden University and the University of Padova from September 2010 under the supervision of Andrea Lucchini in Padova and Hendrik W. Lenstra in Leiden.