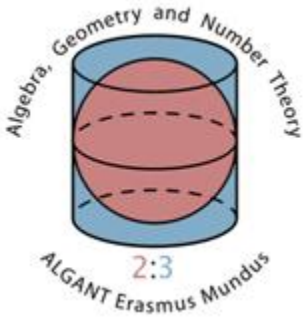
Universiteit Stellenbosch University
Università degli studi di Padova



ALGANT MASTER THESIS

The probabilistic zeta function of the free prosupersolvable group of finite rank

Student:
Giovanni De Franceschi

Advisor:
Andrea Lucchini

Academic year 2013-2014

Contents

1 Introduction

Let G be a group and let $d(G)$ be the minimum cardinality of a generating set for G (e.g. $d(G) = 1$ if and only if G is cyclic). Our question is: given a positive integer k, what is the probability of generating G with k random elements of G?

If G is finite, this probability is defined in the trivial way: it is the ratio between the number of k-tuples generating G and the number of all possible k-tuples of elements of G. For infinite groups, this ratio does not make sense so in order to define a probability on G, we need to define a measure μ on G with the suitable properties: $\mu(G) = 1$, μ is countably additive and invariant under "translations" (i.e. multiplication of subsets of G by elements of G). We will use the Haar measure defined on profinite groups, whose definition starts with the obvious property $\mu(H) = 1/|G : H|$ for $H \leqslant G$ open subgroup. The set of all k-tuples generating a profinite group G is measurable, so it is possible to define our probability $P_G(k)$ for $k \in \mathbb{N}$.

For any group G, it is obvious that $P_G(k) > 0$ only if $k \geq d(G)$. But this condition may be not sufficient. For example: $\mathbb{Z}$ is cyclic, so $d(\mathbb{Z}) = 1$, but there are only two elements that generate $\mathbb{Z}$, namely 1 and -1. So we can think that the probability of generating $\mathbb{Z}$ with one element is $P_{\mathbb{Z}}(1) = 0$; the first integer k such that $P_{\mathbb{Z}}(k) > 0$ is 2, as we can see from observing that asking if two random integers generate $\mathbb{Z}$ is equivalent to asking if they are coprime. For any prime p, the probability that the two integers are not both divisible by p is $\left(1 - \frac{1}{p^2}\right)$; multiplying such expression over all primes p we get $P_{\mathbb{Z}}(2) = \prod_p \left(1 - \frac{1}{p^2}\right) = \zeta(2)^{-1} = \frac{6}{\pi^2} > 0$. Note that in this last argument we spoke about a probability in an abstract intuitive sense, not about an effective probability measure on $\mathbb{Z}$; to do it we need to pass to the profinite completion $\widehat{\mathbb{Z}}$, as we will see below.

If we denote $d^*(G)$ the minimum integer k such that $P_G(k) > 0$, then as an example we have $d^*(\mathbb{Z}) = 2$; but in general case such an integer will not exist. For instance, if G is the d-generated free profinite group, then $P_G(k) = 0$ for any k. In this case we will say that G is not a PFG group, where PFG = "positively finitely generated". Examples of PFG group are the prosolvable finitely generated groups.

If N is an open normal subgroup of G, then the probability $P_G(k)$ can be factorized as $P_G(k) = P_{G/N}(k)P_{G,N}(k)$, where $P_{G,N}(k)$ can be viewed as the probability that a k-tuple generates G given that it generates G modulo N. So $P_{G/N}(k)$ can be computed easily since G/N is a finite group. This suggests a possible infinite factorization of $P_G(k)$: suppose we have a chain of normal subgroups

$$\Sigma : G = N_0 > N_1 > \cdots > N_\mu = 1$$

indexed by countable ordinals such that for any limit ordinal λ we have $\bigcap_{\nu<\lambda} G_\nu = G_\lambda$. We expect that the probability can be rewritten in the form $P_G(k) = \prod_i P_{G/N_{i+1},N_i/N_{i+1}}(k)$, where each factor is the probabilistic function of a finite group, so we can study the convergence of the given infinite product. This is possible under some conditions and after some work.

For example ,there already exist estimations for $d^*(G)$ if G is a free prosupersolvable group of rank $d \geq 2$ (the case where N_i/N_{i+1} is abelian). For example, if $d \geq 2$, and $c_3 = \log_9 48 + \frac{1}{3}\log_9 24$ is the Pálfy-Wolf constant, then $d^*(G) = [c_3(d-1)]+1$ (see [4]). For particular prosolvable groups $d^*(G)$ can be closer to d. For instance, if G is the pronilpotent group of rank d (that is $N_i/N_{i+1} \leqslant Z(G/N_{i+1})$), then $d^*(G) = d+1$. A more general case is the case of metabelian groups: in (Theorem D, [13]) Weigel shows that $d^*(G) \geq 2d + 1$.

In this thesis we ask ourselves what happens in the case where G is prosupersolvable (N_i/N_{i+1} cyclic group). Supersolvability is a weaker property than nilpotency, but it is stronger than solvability, so we expect that $d^*(G)$ is less than $[c_3(d-1)] + 1$. Also, we will see that $P_G(k) = P_{G/\mathrm{Frat}G}(k)$, and since $G/\mathrm{Frat}G$ is metabelian, we have $d^*(G) \leq 2d + 1$; we want to see if we can improve this estimantion and write an exact formula for $P_G(k)$. Moreover we study only the free prosupersolvable group: in fact, any other prosupersolvable group is the epimorphic image of the free prosupersolvable

group of same rank, so its formula involves just some of the factors in the formula for the free case, and convergence in the free case ensures convergence in the general case.

In order to obtain the formula for $d^*(G)$, we will give definitions and properties of the Haar measure, the probabilistic zeta function for groups G, and of the free prosupersolvable groups, and we will introduce some tools such as cohomology of groups, that will be useful in the computation of the formula. The formula will be first computed for the finite case and then generalized to the profinite case. We will not deal with the convergence of the complex function $P_G(s)$, because we are interested to the case where $s = k$ is an integer greater than or equal to $d = d(G)$. Once we have the formula we will have obtained the information about $d^*(G)$.

2 Preliminaries

Let G be a countably based profinite group, $\mathcal{B}$ the smallest family of subsets of G which contains all of the closed subsets, is closed under countable union and complementation. We want to define a measure on G, i.e. a countably additive function $\mu : \mathcal{B} \to \mathbb{R}_{\geq 0}$. μ is called *Haar measure* on G if:

- $\mu(G) = 1$;
- for any $B \in \mathcal{B}$, $g \in G$ we have $\mu(gB) = \mu(B) = \mu(Bg)$.

The group G becomes a probability space $(G, \mathcal{B}, \mu)$.

We can see by construction that the Haar measure exists and is unique. Firstly if $H \trianglelefteqslant G$ is open, then $|G : H| < \infty$. Writing G as finite union of disjoint cosets of H we have $G = Ht_1 \cup \cdots \cup Ht_r$ with $r = |G : H|$, so $1 = \mu(G) = \mu(Ht_1 \cup \cdots \cup Ht_r) = \mu(Ht_1) + \cdots + \mu(Ht_r) = r\mu(H) \Rightarrow \mu(H) = \frac{1}{|G:H|}$. Now we can determine the measure of any open subset A. If A is finite union of the kind $A = H_1 g_1 \cup \cdots \cup H_t g_t$ with H_i open normal subgroup and $g_i \in G$, then A is disjoint union of cosets of $H_1 \cap \cdots \cap H_t$ and then $\mu(A) = \frac{m}{|G:H_1 \cap \cdots \cap H_t|}$ for a suitable integer m. If A is countable union of subsets $(H_i g_i)_{i \in \mathbb{N}}$, then $\mu(A)$ can be defined as

$$\mu(A) = \lim_{j \to \infty} \mu \left(\bigcup_{i \leq j} H_i g_i \right);$$

note that such limit is well-defined because the sequence into the limit is increasing.

Finally, if C is closed, it follows $\mu(C) = 1 - \mu(G \setminus C)$.

Another equivalent construction allows to give a definition of μ without passing through open subsets. If $\mathcal{N}$ is the set of all open normal subgroups of G and $(N_i)_{i \in \mathbb{N}}$ is a filtering descending chain in $\mathcal{N}$, then for any closed subgroup X of G, $X = \bigcap_{N \in \mathcal{N}} XN = \bigcap_{i \in \mathbb{N}} XN_i$; hence $\mu(X) = \inf_i \mu(XN_i) \geq \inf_{N \in \mathcal{N}} \mu(XN) \geq \mu(X)$, so we have the equality everywhere. Now XN is union of $|XN/N|$ cosets of N, so $\mu(XN) = \mu(N)|XN : N| = \frac{|XN:N|}{|G:N|}$ and then we can define

$$\mu(X) := \inf_{N \in \mathcal{N}} \frac{|XN : N|}{|G : N|}.$$

Now come back to our probability $P_G(k)$. If G is a profinite group, $k \in \mathbb{N}$, denote

$$\Phi(G, k) = \{(g_1, \ldots, g_k) \in G^k \, : \, \langle g_1, \ldots, g_k \rangle = G\}.$$

Observe that if $(g_1, \ldots, g_k) \notin \Phi(G, k)$, then $\overline{\langle g_1, \ldots, g_k \rangle}$ is contained in a maximal subgroup M of G, and this is possible if and only if $(g_1, \ldots, g_k) \in M^k$. Thus $\Phi(G, k) = G^k \setminus \bigcup M^k$, where the union runs over all maximal subgroups of G. This shows that $\Phi(G, k)$ is closed in G^k, so it is measurable and we can define $P_G(k) := \mu(\Phi(G, k))$.

Lemma 1 *Let G be a profinite group. Then*

$$d(G) = \inf_{N \trianglelefteqslant G \text{ open}} d(G/N).$$

Proof: for every $N \trianglelefteqslant G$ we have $d(G) \leq d(G/N)$, because if some elements generate G, then they generate also G modulo N. For every N, say $\Omega_N = \{(g_1, \ldots, g_d) \in G^d \, : \, \langle g_1, \ldots, g_d \rangle N = G\} \neq \varnothing$ (where $d = d(G)$). Ω_N is closed since it is a union of cosets of N^d in G^d. If $N \leqslant M$, then $\Omega_N \subseteq \Omega_M$, so $\varnothing \neq \Omega_{N_1 \cap N_2} \subseteq \Omega_{N_1} \cap \Omega_{N_2}$. By compactness

$$\bigcap_{N \trianglelefteqslant G \text{ open}} \Omega_N \neq \varnothing,$$

so it contains a certain $(g_1, \dots, g_d)$. By definition $\langle g_1, \dots, g_d \rangle N = G$ for every N, so $\overline{\langle g_1, \dots, g_d \rangle} = G$, as we wished. $\square$

Theorem 1 *Let G be a profinite group. Then*

$$P_G(k) = \inf_N P_{G/N}(k),$$

where N runs over all open normal subgroups of G. Moreover if $\{N_i\}$ is a basis of open normal subgroups for G, then $P_G(k) = \inf_i P_{G/N_i}(k)$.

Proof: G/N is finite, so $P_{G/N}(k)$ is simply the number of all k-tuples generating G/N over $|G/N|^k$. Clearly if a k-tuple in G generates G, then the respective k-tuple in G/N generates G/N, so $P_G(k) \leq P_{G/N}(K)$; it follows $P_G(k) \leq \inf P_{G/N}(k)$. If such infimum is zero, then $P_G(k) = 0$ too. Suppose $\inf P_{G/N}(k) > 0$. Any factor G/N can be generated by k elements, therefore so can G by Lemma 1. G has only finitely many open normal subgroups N of a given index, so it has only countably many open normal subgroups. So we can find a sequence $\{M_i\}$ that is a basis for G, and WLOG $M_i \geqslant M_{i+1}$ for every i. Let S be the set of all k-tuples generating G and S_i the set of all k-tuples generating G module M_i. $S = \bigcap S_i$ and $S_i \supseteq S_{i+1}$, so $P_G(k) = \mu(S) = \inf \mu(S_i) = \inf \lim \mu(S_i)$. For every N open normal subgroup, N contains some M_i (definition of basis), so $P_{G/N}(k) \geq P_{G/M_i}(k)$, so $P_G(k) = \inf P_{G/N}(k)$. Finally, if $\{N_i\}$ is any subgroup basis, then every $N \trianglelefteqslant G$ open contains some N_i, so $P_{G/N}(k) \geq P_{G/N_i}(k)$ and then $P_G(k) = \inf P_{G/N_i}(k)$. $\square$

2.1 Probabilistic zeta functions

We want to compute the probability that two random integers are coprime, say it p. These two numbers generates a subgroup $n\mathbb{Z}$ of $\mathbb{Z}$, with $n \neq 0$ (this case has probability 0, so it can be omitted). The probability that the two numbers belong to $n\mathbb{Z}$ is $1/n^2$ and in this case the probability that they generate $n\mathbb{Z}$ is p, since $n\mathbb{Z} \cong \mathbb{Z}$. Since they surely generate a subgroup $n\mathbb{Z}$, we have $p(\sum 1/n^2) = 1 \Rightarrow p = \zeta(2)^{-1} = 6/\pi^2$.

In another way, two integers are coprime if for every prime q they are not both divisible by q, and this last probability is $(1 - 1/q^2)$. By Chinese Remainder Theorem the total probability is given by the product over all primes q, that is $p = \prod(1 - 1/q^2) = \zeta(2)^{-1}$.

We can do similar considerations for any integer k. In the case $k = 1$ the probability is 0 (the probability that an integer is coprime with itself is the probability that it generates $\mathbb{Z}$), and by $0 = \prod(1 - 1/q)$, this says that there are infinitely many primes and $\sum 1/q$ diverges.

The discussion can be extended to $\widehat{\mathbb{Z}}$ and then to any free abelian group of finite rank. The result we obtain is that the probability that k elements generate G is $\zeta_G(k)^{-1}$, where ζ_G is the *subgroup zeta function*

$$\zeta_G(k) = \sum_{n=1}^{\infty} \frac{c_G(n)}{n^s},$$

where $c_G(n)$ is the number of subgroups of G of index n.

These examples suggest us to find, for every PFG group G, a function $\zeta(k)$ interpolating $P_G(k)$, an analytic function defined in some right half-plane of the complex plane such that $\zeta(k) = 1/P_G(k)$. For example, if G is a pro-p-group of rank r, then $\zeta(k) = \zeta^{(p)}(k) \cdots \zeta^{(p)}(k - r + 1)$ for every $k \geq r + 2$, with $\zeta^{(p)}(k) = (1 - 1/p^k)$.

Now come back to the formula $P_G(k)$. We saw that it can be written as

$$P_G(k) = \sum_M \frac{1}{|M|^k} - \sum_{M,L} \frac{1}{|M \cap L|^k} + \sum_{M,N,L} \frac{1}{|M \cap N \cap L|^k} - \cdots, \tag{1}$$

where every sum runs over all maximal subgroups of G. This expression makes sense only if each of the infinitely many sums occurring in it converges, and in this case we rearrange the series as follows. Choose a descending subgroup basis $\{N_i\}$ of G. Let X_i be the set of all maximal subgroups containing N_i, so that $X_i \subseteq X_{i+1}$ for every i. Then $P_G(k)$ is the limit for $i \to \infty$ that a random k-tuple is not contained in one of the maximal subgroups in X_i. This probability is a finite sum consisting in all terms of (1) involving only maximal subgroups of X_n, and the limit of this sum can be formally rearranged in the form

$$P_G(k) = \sum_H \frac{\mu(H)}{|G : H|^k}, \tag{2}$$

for some integer coefficients $\mu(H)$, where H runs over all subgroups of finite index of G, these being ordered starting by the maximal subgroups of X_1 and every their intersections, then the subgroups of X_2 and their intersections, and so on. The group G is included, with coefficient 1. Thus a candidate for $P_G(s)$ is exactly the series (2), observed the first time by P. Hall, with the above insection of brackets and k replaced by a complex variable s. Later we will not be interested to the brackets because in the case of prosolvable groups the convergence is absolute (see [15]). We will refer to this series as the *series associated to* $\{N_i\}$.

We can just say something about the coefficients $\mu(H)$. Since the series (2) is a rearrangement of (1), then we can say that:

1. a subgroup H can occours in (2) with nonzero coefficient $\mu(H)$ if and only if H can be written as intersection of maximal subgroups of G;
2. in such case $\mu(H)$ is the difference between the number of way to write H as intersection of evenly many maximal subgroups of G and the number of way to write H as intersection of oddly many maximal subgroups of G.

Now recall the Möbius function for groups μ_G, defined as follows: $\mu_G(G) = 1$ and for every proper subgroup $H \leqslant G$ of finite index we have $\sum_{K \geqslant H} \mu_G(K) = 0$. This defines μ_G uniquely by recursion. Notice that for $G = \mathbb{Z}$, we have $\zeta_{\mathbb{Z}}(k) = \sum_n \frac{\mu(n)}{n^k} = \zeta(k)^{-1}$.

First, let G be a finite group and N a minimal normal subgroup of G. If $N \leqslant \mathrm{Frat}(G)$, then $P_G(k) = P_{G/N}(k)$ for every k. Indeed if $M < G$ maximal, then M/N is maximal in G/N and $|G/N : M/N| = |G : M|$; moreover for any $M_1, \ldots, M_r$ maximal subgroups $M_1/N \cap \cdots \cap M_r/N = (M_1 \cap \cdots \cap M_r)/N$, so the formula (1) remains unchanged. Conversely, if $N \not\leqslant \mathrm{Frat}(G)$, then $P_G(k) = P_{G/N}(k) P_{G,N}(k)$, where

$$P_{G,N}(k) = 1 + \sum_r (-1)^r \sum_{i_1 < \cdots < i_r} \varepsilon_{i_1,\ldots,i_r} |G : M_{i_1} \cap \cdots \cap M_{i_r}|^{-k}, \tag{3}$$

where the M_i are the maximal subgroups of G and $\varepsilon_{i_1,\ldots,i_r}$ is 1 or 0 according to whether $N(M_{i_1} \cap \cdots \cap M_{i_r}) = G$ or not. Note that by the expression $P_{G,N}(k) = P_G(k)/P_{G/N}(k)$, $P_{G,N}(k)$ can be seen as the probability that a random 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 of $P_G(k)$ as a product, indexed on

the non-Frattini factors of G. Now let G be a profinite group, take $\{N_i\}$ a descending subgroup basis and refine it to a chief series. For each factor $N = R/S$ in the chief series, express $P_{G/S}(k)$ as above. In the expression for $P_{G/S,N}(k)$ we can, without changing its value, replace maximal subgroups of G/S by the corresponding maximal subgroups of G. Since $P_G(k) = \lim P_{G/S}(k)$, this expresses $P_G(k)$ as an infinite product, indexed by the set of non-Frattini factors in our chief series (recall that R/S is a Frattini factor if $R/S \leqslant \mathrm{Frat}(G/S)$). The candidate for our probabilistic zeta function is $P_G(s)$, with the complex variable s instead of k. The subgroups H that occur inside the factors of the product are the maximal intersections H such that $HR = G$, where R/S is a factor in the chief series and S is the first term of the chief series that is contained in H. The factor R/S is determined by H, but H may occur more than one in the corresponding factor of the product, because it may be expressed in more ways as a maximal intersection. So H occurs with coefficient $\mu(H)$, described in the same way as above, the Möbius function of the group G. All the factors in the product are probabilities, so they lie between 0 and 1, and writing the product as $\prod(1 + x_n)$ its convergence is equivalent to 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 (1), but in which just some of the maximal intersections occur.

Proposition 1 *Given a descending normal subgroup basis, the associated series and the product 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 the 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, we have that both P_i 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. □

Now let's see the solvable and prosolvable cases.
A subgroup H occurs in the formula for $P_{G,N}(k)$ only if it is a maximal subgroup complementing N, so $P_{G,N}(k) = 1 - c(N)/|N|^k$, where $c(N)$ is the number of complements of N. Therefore, the infinite product associated to a chief series of a prosolvable group is

$$P_G(k) = \prod_N \left(1 - \frac{c(N)}{|N|^k}\right), \tag{4}$$

where the product running over all complemented chief factors in the chief series.

Theorem 2 *Let G be a finitely generated prosolvable group. For any chief series of G, the associated product converges absolutely in some half plane, and all the functions $P_G(s)$ obtained in this way have the same domain of absolute convergence and define the same function in this domain. This function is also defined by the associated series.*

Proof: the product (4) (with s replacing k) converges if and only if the series $\sum c(N)/|N|^s$ does. Since the coefficients are positive, any rearrangement has no influence on the absolutely convergence, so we can collect terms with the same denominator. The coefficient of $1/n^s$ is $\sum_{|N|=n} c(N)$. If a given chief series, different factors are complemented by different maximal subgroups, and each maximal subgroup complements some chief factor, therefore $\sum_{|N|=n} c(N) = m_n(G)$, so our series if $\sum_n m_n(G)/n^s$ (where $m_n(G)$ is the number of maximal subgroups of G of index n). This series does not depend by the choice of the subgroup basis and of the chief series, so all products (4) have the same domain of absolute convergence, which is a right half plane. Let $s(G) = \limsup((\log m_n(G))/\log n) = \inf\{s : m_n(G) \leq Cn^s, \text{ for some } C\}$ (for all subgroups for which it makes sense). If $s > s' > s(G)$, then $m_n(G) \leq Cn^{s'}$ for some C, so the series $\sum m_n(G)/n^{s+1}$ converges. On the other hand, if $s < s(G)$, then for infinitely

many n's we have $m_n(G) \geq n^s$ and the series $\sum m_n(G)/n^s$ does not converge. Thus the abscissa of absolute convergence lies between $s(G)$ and $s(G)+1$.

If we have two chief series corresponding to the same subgroup basis, then the argument of Proposition 1 shows that the associated products are equal whenever they both converge. Next, if we replace a subgroup basis by a subsequence of it, we can use the same chief series for both bases, so we get the same product and the same function. Finally, if we have two subgroup bases, say $\{N_i\}$ and $\{M_j\}$, then by passing in both to subsequences we may assume that $N_{i+1} \leqslant M_i \leqslant N_i$ for every i, and then we can combine them to one basis such that both are subsequences of it. This shows that all products (4) define the same function in the domain of common convergence of all of them, and in particular in the half plane of absolute convergence. Proposition 1 shows that the associated series also defines the same function in this domain. $\square$

3 Prosupersolvable groups

If G is a group, denote with $\widehat{G}$ its profinite completion

$$\widehat{G} = \varprojlim G/N,$$

where N runs over all the normal subgroups of finite index of G. More in general, if $\mathcal{C}$ is a class of groups that is closed under intersection, factor groups and products, the *pro-$\mathcal{C}$-completion* of G is $\varprojlim G/N$, where N runs over all normal subgroups of G such that $G/N \in \mathcal{C}$.

Recall that the *Frattini subgroup* of a profinite group G, denoted by $\mathrm{Frat}G$ is defined as the intersection of all closed maximal subgroups of G, and it is easy to see that if $\varphi : G_1 \to G_2$ is an epimorphism, then $\mathrm{Frat}(\varphi(G_1)) \subseteq \mathrm{Frat}G_2$.

Proposition 2 *Let $\{G_i,\, i \in I\}$ be an inverse system of profinite groups for a direct set $(I, \leq)$. Suppose that the canonical maps $\varphi_{ij} : G_i \to G_j$ are epimorphisms. Then*

$$\mathrm{Frat}(\varprojlim G_i) = \varprojlim \mathrm{Frat}G_i.$$

Proof: put $G = \varprojlim G_i$ and $\pi_i : G \to G_i$ the canonical epimorphism. Since $\pi_i(\mathrm{Frat}G) \subseteq \mathrm{Frat}G_i$ and $\mathrm{Frat}G_i = \varprojlim \pi_i(\mathrm{Frat}(G))$ we get $\mathrm{Frat}(G) \subseteq \varprojlim \mathrm{Frat}G_i$. Conversely, let $x = (x_i)_i \in \varprojlim \mathrm{Frat}G_i$ and suppose $x \notin \mathrm{Frat}G$. Then there is a maximal open subgroup M of G with $x \notin M$. Hence there is some $i \in I$ with $x_i \notin \pi_i(M)$. Since $\pi(M)$ is maximal in G_i, one has $x_i \notin \mathrm{Frat}G_i$, contradiction. Thus $x \in \mathrm{Frat}G$, i.e. $\varprojlim \mathrm{Frat}G_i \subseteq \mathrm{Frat}G$. □

Recall that a finite group is supersolvable if there exists a *chief series*

$$1 = N_l \lhd N_{l-1} \lhd \cdots \lhd N_1 \lhd N_0 = G$$

such that N_i is normal in G and N_i/N_{i+1} is cyclic for every i. Clearly supersolvable groups are solvable, and it's easy to check that subgroups and factor groups of supersolvable groups are supersolvable. The factor groups N_i/N_{i+1} are called *chief factors* of G. Another characterization of supersolvable groups is given by the following:

Proposition 3 *Let G be a finite supersolvable group. Then:*

(a) *if N is a minimal normal subgroup of G, then $|N| = p$ for some prime p (in particular N is abelian);*

(b) *if M is a maximal subgroup of G, then $|G : M| = p$ for some prime p.*

Proof: (a) for every i we have $N \cap N_i \trianglelefteq G$, so by minimality of N, necessarly $N \cap N_i = 1$ or $N \cap N_i = N \Rightarrow N \subseteq N_i$. Let i be the maximal integer such that $N \subseteq N_i$, so $N \cap N_{i+1} = 1$. The homomorphism $N \hookrightarrow N_{i-1} \twoheadrightarrow N_{i-1}/N_i$ has kernel $N \cap N_i = N$, so N embeds into N_{i-1}/N_i, that is a finite cyclic group. Then N is also a finite cyclic group, and its order is necessarly p, otherwise it would have a characteristic nontrivial subgroup, against the minimality of N in G.

(b) Work by induction on $|G|$. Let N be a minimal normal subgroup of G. If $N \subseteq N$, then M/N is maximal in G/N, whose order is less than $|G|$, so by induction $|G : M| = |G/N : M/N| = p$ prime. Suppose $N \nsubseteq M$. Then $M < NM$ and by maximality $MN = G$. $N \cap M$ is normal in M and in N too (because N is abelian by point (a)), so $M \cap N$ is normal in $MN = G$ and by minimality of N we have $M \cap N = N$ (so $N \leqslant M$ as in the previous case) or $M \cap N = 1$, and in this case $|G : M| = |N| = p$ by point (a). □

A *prosupersolvable group* is a projective limit of finite supersolvable groups. In this case G is supersolvable if and only if every maximal closed subgroup of G has prime index.

Let's fix the notations. Let π be a set of prime numbers and π' the set of all prime numbers not contained in π. We say that a supernatural number α is a *π-number* if the prime numbers dividing α are in π. A closed subgroup H of G is a *π-subgroup* if the order of H is a π-number. Any maximal π-subgroup H is called *Syolw π-subgroup* of G and it is called a *Hall π-subgroup* if it is a Sylow π-subgroup of G and $|G : H|$ is a π'-number. If G is prosupersolvable (and hence prosolvable), every Sylow π-subgroup is a Hall π-subgroup, and any two of them are conjugate.

Proposition 4 *Let π be a set of all prime numbers greater than a fixed natural number n and G a prosupersolvable group. Then*

1. *there is a unique normal Sylow π-subgroup K of G;*
2. *there is a split exact sequence of prosupersolvable groups*

$$1 \longrightarrow K \longrightarrow G \xrightarrow{\varphi} H \longrightarrow 1,$$

where φ is an open map (and then G is the topological direct semiproduct of K and H) and H is a Sylow π'-subgroup of G.

Proof: for each U open normal subgroup of G, let K_U be the normal Sylow π-subgroup of G/U. Set $K = \varprojlim K_U$. Then K is a normal Sylow π-subgroup of G. Now let H be a Syolw π'-subgroup such that $G = KH$. Then G is, as abstract group, the semidirect product of K and H. Since all the groups involved are compact, G is also the topological semidirect product of K and H. In particular G/K and H are topologically isomorphic and φ is open. □

For example: if $\{p_1, p_2, \dots\}$ is the set of primes dividing $|G|$, then we can choose a chief series $G = N_0 \triangleright N_1 \triangleright \cdots$ such that the orders of the chief factors are orderred: $|N_0 : N_1| = p_1$, $|N_1 : N_2| = p_2$, etc.

Proposition 5 *Let G be a profinite group, H a normal Hall π-subgroup of G. Then* $\mathrm{Frat}H = H \cap \mathrm{Frat}G$.

Proof: by Proposition 2 we may assume G finite. Since $\mathrm{Frat}H \subseteq \mathrm{Frat}G$, we have $\mathrm{Frat}H \subseteq H \cap \mathrm{Frat}G = N \trianglelefteqslant G$. We may assume $\mathrm{Frat}H = 1$ (otherwise we reason with $G/\mathrm{Frat}H$), so that we have to show $N = 1$. Since N is a normal nilpotent subgroup of H, it is contained in the Fitting subgroup of H. But $\mathrm{Fit}H$ is abelian because $\mathrm{Frat}H = 1$. So N is abelian, and since $\mathrm{Frat}H = 1$, H splits over N. Thus G splits over N. Say $G = NL$ with $N \cap L = 1$. If $L \neq G$, then $L \subseteq M$ for a maximal subgroup $M < G$. Then $G = NM = M$, that is impossible ($N \subseteq \mathrm{Frat}G$). Hence $L = G$ and $N = 1$. □

In particular, if G is prosupersolvable whose order is divisible by finitely many primes and p is the largest of these, then by Proposition 4, G has a unique Sylow p-subgroup P and by the last proposition $\mathrm{Frat}P = P \cap \mathrm{Frat}G$.

Theorem 3 *Let G be a supersolvable group whose order is divisible by only finitely many primes $p_1, \dots, p_r$. Then G is topologically finitely generated if and only if* $\mathrm{Frat}G$ *is open.*

Proof: every maximal subgroup of G has prime index, and in particular it is open. Suppose that G is topologically finitely generated; then for each prime p dividing the order of G, there are only finitely many open subgroups of index p. Therefore $\mathrm{Frat}G$ is an intersection of finitely many open subgroups, and thus it is open. The converse is obvious: if $\mathrm{Frat}G$ is open, then $G/\mathrm{Frat}(G)$ is finite and then $G = \overline{\langle X \cdot \mathrm{Frat}G \rangle}$ for a finite subset X. $\square$

Corollary 1 *Let G be a topologically finitely generated prosupersolvable group. Then for each prime number p, every Sylow p-subgroup of G is topologically finitely generated.*

Proof: let p be a prime number and let π be the set of all prime number greater than p. With the notation of Proposition 4, π' is a finite set, so $\mathrm{Frat}H$ is open in H by Theorem 3. Let S_p be the unique Sylow p-subgroup of H. By Proposition 5 $\mathrm{Frat}S_p = S_p \cap \mathrm{Frat}H$, so $\mathrm{Frat}S_p$ is open in S_p, and hence S_p is topologically finitely generated. Finally S_p is also a Sylow p-subgroup of G. $\square$

4 Free pro-$\mathcal{C}$-groups

Denote with $\mathcal{C}$ a class of finite groups which is closed under subgroups and direct products. We will be interested to the case $\mathcal{C} = \{$ supersolvable groups $\}$.

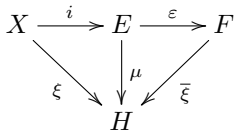
The *free pro-$\mathcal{C}$-group* of rank n is a pro-$\mathcal{C}$-group F together a map $j : X = \{1, \dots, n\} \to F$ satisfying the following universal property: for any other profinite group G and map $\alpha : X \to G$ there exists a unique (continuous) homomorphism $\overline{\alpha} : F \to G$ such that $\alpha = \overline{\alpha} j$.

It's easy to see that the free pro-$\mathcal{C}$-group, if it exists, is unique up to isomorphisms. Indeed if F_1 and F_2 are two pro-$\mathcal{C}$-groups on X with the respective maps j_1 and j_2, then the universal property for F yields a homomorphism $\alpha : F_1 \to F_2$ such that $j_2 = \alpha j_1$; analogously there is a homomorphism $\beta : F_2 \to F_1$ such that $j_1 = \beta j_2$. Thus $j_1 = \beta j_2 = \beta(\alpha j_1) = (\beta\alpha) j_1$ and by injectivity of j_1 it follows $\beta\alpha = \mathrm{id}_{F_1}$. Analogously $\alpha\beta = \mathrm{id}_{F_2}$ and then F_1 and F_2 are isomorphic.

The following proposition gives a proof of the existence of free pro-$\mathcal{C}$-groups based on free abstract group:

Proposition 6 *Let E be the free abstract group on X. Then the free pro-$\mathcal{C}$-group F is the profinite completion of E together with the map $j : x \mapsto (Ui(x))_{U \in I}$, where $I = \{N \trianglelefteq E \text{ closed } : E/N \in \mathcal{C}\}$ and $i : X \to E$ is the inclusion map.*

Proof: if ε is the canonical map from E to its completion F, then $j = \varepsilon i$. Let $\xi : X \to H$ be a map into a $\mathcal{C}$-group H. By the universal property of the free abstract group, there is a unique homomorphism $\mu : E \to F$ such that $\xi = \mu i$, and since X is finite, then $\ker \mu \in I$ and μ is continuous with respect to the topology on E having I as a base of open neighborhoods of 1. By the universal property of the pro-$\mathcal{C}$-completion there is a map $\overline{\xi} : F \to X$ such that $\mu = \overline{\xi}\varepsilon$. Then $\xi = \mu i = \overline{\xi}\varepsilon i = \overline{\xi} j$.



Now if $\overline{\xi}_1 : F \to H$ is another homomorphism such that $\overline{\xi}_1 j = \xi$, then $(\overline{\xi}_1 \varepsilon) i = \xi$, so by the universal property of E we have $\overline{\xi}_1 \varepsilon = \mu$. But $\mu = \overline{\xi}\varepsilon$, so by the universal property of the completion F we have $\overline{\xi}_1 = \overline{\xi}$. $\square$

In particular, any d-generated profinite $\mathcal{C}$-group G is epimorphic image of the free pro-$\mathcal{C}$-group of rank d: indeed if $G = \langle g_1, \dots, g_d \rangle$ we take $X = \{1, \dots, d\}$ and $\xi : X \to G$ defined by $\xi(i) = g_i$. Then if F is the free pro-$\mathcal{C}$-group of rank d there exists a unique homomorphism $\overline{\xi} : F \to G$ such that $\xi = \overline{\xi} j$. In particular $\overline{\xi}(j(i)) = \xi(i) = g_i$ for any $1 \le i \le d$, so $\{g_1, \dots, g_d\} \subseteq \operatorname{im} \overline{\xi}$ and then $\overline{\xi}$ is an epimorphism. This property will be useful when we compute the formula $P_G(s)$: if G is a d-generated profinite group, then it is epimorphic image of F, so the factors comparing in the product of $P_G(s)$ will be some of the factors comparing in the product of $P_F(s)$ and then we can just study the convergence of $P_G(s)$ for G free pro-$\mathcal{C}$-group of rank d.

5 The formula for $P_G(k)$

Now we will find the formula for $P_G(k)$ with G free prosupersolvable group of rank d. This formula derives from the finite case.
There are several approaches to the problem: in this context we pass from the eulerian function $\phi_G(k)$, that is simply the cardinality of the set of k-tuples which generate G (by definition $P_G(k) = \phi_G(k)/|G|^k$ for any k) and before we need to introduce some tools of cohomology of groups.

The passage from the finite case to the profinite one requires the crown theory. The result won't give a function in general (because the infinite product does not converge in general), but we will focus on the prosolvable group, and in this case the product converges for any integer t sufficiently large. From this we can obtain the formula for free prosupersolvable groups, that is particularly simple because the modules A comparing in the product are cyclic of prime order, and make considerations about convergence.

5.1 The formula in finite case

5.1.1 Preliminaries on group cohomology

In this section we will give some results on group cohomology that will serve in next sections. For a more complete introduction about the cohomology group, see for example [8].

Let G be a finite group, A a G-module with the action of G $(a, g) \mapsto ag \in A$ for $a \in A$ and $g \in G$. We use the additive notation for the abelian group A. Define the following G-submodules of A:

- $F_G(A) = \{a \in A : ag = a \text{ for all } g \in G\}$;
- $T_G(A) = \{T_G(a) : a \in A\}$, where $T_G(a) = \sum_{g\in G} ag$ is the trace of a.

Below we will write $F(A) = F_G(A)$ and $T(A) = T_G(A)$. If A is any abelian group and A^* is the set of all functions (not necessarly homomorphism) of G in A, then A^* can be made an abelian group defining

$$(\phi_1 + \phi_2)(g) = \phi_1(g) + \phi_2(g), \quad g \in G,\ \phi_1, \phi_2 \in A^*.$$

Moreover A^* is a G-module with the action:

$$\phi g : x \mapsto \phi(xg^{-1}).$$

If A is a G-module, define the position $^\circ : A \to A^*$ defined by $a \mapsto a^\circ : g \mapsto ag^{-1}$ for $a \in A$ and $g \in G$. Then $^\circ : A \to A^*$ is a G-monomorphism. In fact for every $a \in A$ and $g, x \in G$, $(ag)^\circ(x) = agx^{-1} = a^\circ(xg^{-1}) = (a^\circ g)x$. The injectivity follows by $\ker{}^\circ = 0$, because $a^\circ(x) = 0$ for every $x \in G$ if and only if $a = 0$. Moreover if $B = \{\phi \in A^* : \phi(1) = 0\}$, then $A^* = A^\circ \oplus B$ (this is a direct sum of groups, not of G-modules: B is not a G-module in general).

Now let's say *separable resolution* of A the following sequence

$$X_0 = A \xrightarrow{i_0} X_1 \xrightarrow{i_1} X_2 \xrightarrow{i_2} X_3 \xrightarrow{i_3} \cdots$$

defined as follows: $X_0 = A$, $X_1 = A^*$ and $i_0 = {}^\circ$; now for recurrence $A_n = X_n/\operatorname{Im} i_{n-1}$, $X_{n+1} = A_n^*$ and $i_n = {}^\circ$ on A_n. It is not difficult to see that $\operatorname{Im} i_{n-1} = \ker i_n$ for every n. Finally let A be a G-module. Put $H^0(G, A) = F(A)/T(A)$. For every $n \in \mathbb{N}$, say

$$H^n(G, A) = H^0(G, A_n).$$

The groups $H^n(G,A)$ are the *cohomology groups* of A.

Example: let's describe the group $H^1(G,A)$. By definition $H^1(G,A) = F(A^*/A^\circ)/T(A^*/T^\circ)$. Write for convenience $F(A^*/A^\circ) = D/A^\circ$, $T(A^*/A^\circ) = E/A^\circ$ and $F = \{\phi \in A^* : 1\phi = 0\}$. We have the following scheme

$$\begin{array}{ccccccc} A^\circ & \longrightarrow & E & \longrightarrow & F & \longrightarrow & A^* \\ | & & | & & | & & | \\ 0 & \longrightarrow & B = E \cap F & \longrightarrow & Z = D \cap F & \longrightarrow & F \end{array}$$

and then $H^1(G,A) \cong Z/B$. Explicitely we have

$$\begin{aligned} A^\circ &= \{\phi \in A^* : \phi(x) = ax^{-1}\} = \{\phi \in A^* : \phi(x)x = \phi(1)\}; \\ D &= \{\phi \in A^* : \phi - \phi g \in A^\circ \text{ for every } g \in G\} \\ &= \{\phi \in A^* : \phi(x)x - (\phi g)(x)x = \phi(1) + (\phi g)(1) \text{ for every } g \in G\} \\ &= \{\phi \in A^* : \phi(x) - \phi(xg^{-1}) = \phi(1)x^{-1} + \phi(g^{-1})x^{-1} \text{ for every } g \in G\}; \\ D \cap F &= \{\phi \in A^* : \phi(x) - \phi(xg^{-1}) = \phi(g^{-1})x^{-1}\} \end{aligned}$$

and replacing $\phi(x)$ with $\phi(x^{-1})$ we can write $Z = D \cap F = \{\phi : A^* : \phi(xy) = \phi(x)y + \phi(y)\} = \mathrm{Der}(G,A)$.
Let's check that $H^1(G,A^*) = 0$. If $\phi \in F(A^*)$, then $(\phi g)(x) = \phi(xg^{-1}) = \phi(x)$ for any $g, x \in G$, i.e. $\phi = \phi_0$ is constant. So if we take $\psi \in A^*$ defined by $\phi(1) = \phi_0$ and $\psi(x) = 0$ for $x \neq 1$, then $T(\psi) = \phi_0 = \phi$, so $\phi \in T(A^*)$. Then $T(A^*) = F(A^*)$.
It follows that $E = A^\circ + T(A^*) = A^\circ + F(A^*) = \{\phi \in A^* : \phi(x) = ax^{-1} + b\}$ for some $a, b \in A$. So $E \cap F = \{\phi \in A^* : \phi(x) = ax^{-1} - a\}$ and again replacing $\phi(x)$ with $\phi(x^{-1})$ we can write $B = \{\phi \in A^* : \phi(x) = ax - a\}$.
In future it will be necessary to write $Z = Z^1(G,A)$ and $B = B^1(G,A)$.

Example: with similar computations one can check that $H^2(G,A) = Z^2(G,A)/B^2(G,A)$, where

$$\begin{aligned} Z^2(G,A) &= \{\phi \in A^{**} : \phi(y,z) + \phi(x,yz) = \phi(xy,z) + \phi(x,y)z \text{ for every } x,y,z \in G\} \\ B^2(G,A) &= \{\phi \in A^{**} : \phi(x,y) = \phi_1(y) - \phi_1(xy) + \phi_1(x)y \text{ for some } \phi_1 \in A^*\}. \end{aligned}$$

Proposition 7 *Let A be a G-module. Then for every $n \in \mathbb{Z}$:*

(i) $\exp H^n(G,A) \big| |G|$;

(ii) $\exp H^n(G,A) \big| \exp A$.

Proof: (i) for any G-module X, the exponent of $F(X)/T(X)$ divides $|G|$: indeed for any $a \in F(X)$, $|G|a = \sum_{g \in G} ag = T(a) \in T(X)$. The conclusion follows immediatly.

(ii) $H^n(G,A) = F(A_n)/T(A_n)$, so it sufficies to prove that $\exp A_n \big| \exp A$, and it is sufficient to show that $\exp A_1 \big| \exp A$ (the others follows by induction). If $r = \exp A$, $ra = 0$ for every $a \in A$, then for every $\phi \in A^*$ we have $(r\phi)(g) = (\phi + \cdots + \phi)(g) = \phi(g) + \cdots + \phi(g) = r\phi(g) = 0$ for any $g \in G$, so $\exp A_1 \big| \exp A$. $\square$

In the following we use the multiplicative notation for the G-modules A.

Theorem 4 *Let A be a normal abelian subgroup of H and let G be a finite subgroup of H such that $AG = H$ and $A \cap G = 1$. A is a G-module by taking $a^g = g^{-1}ag$ for every $a \in A$ and $g \in G$. Then $|H^1(G, A)|$ is equal to the number of conjugacy classes of complements of A in H.*

Proof: let $\overline{G}$ be a complement of A in H. We can write $\overline{G} = \{x\phi(x) : x \in G, \phi(x) \in A\}$, where $\phi(x)$ is the unique element of A such that $x\phi(x) \in \overline{G}$. We have $x\phi(x)y\phi(y) = xy\phi(x)^y\phi(y) \in \overline{G}$, but also $xy\phi(xy) \in \overline{G}$, so it follows $\phi(xy) = \phi(x)^y\phi(y)$ and then $\phi \in Z^1(G, A)$. Now if $\overline{G}$ and G are conjugate, we have, for any $x \in G$, $x\phi(x) = a^{-1}xa = xa^{-x}a$ for a suitable $a \in A$, and this shows $\phi \in B^1(G, A)$. The conclusion follows immediatly. $\square$

Let A be a G-module. An *extension* of A is an exact sequence $\mathcal{H}$ of groups

$$1 \longrightarrow A \xrightarrow{i} H \xrightarrow{j} G \longrightarrow 1$$

where $A \leqslant H$ and i is the inclusion. A function $r : G \to H$ such that $jr = 1_G$ is called *retraction* (it always exists because j is surjective). In this case we take $\phi_{\mathcal{H},r}(x, y) = r(xy)^{-1}r(x)r(y)$ for $x, y \in G$. We say that $\mathcal{H}$ is a *split extension* (or that r splits $\mathcal{H}$) if r is an homomorphism.

Theorem 5 *Let A be a G-module, $\mathcal{H}$ an extension of A. Then:*

(a) *for any retraction r, $\phi_{\mathcal{H},r} \in Z^2(G, A)$;*

(b) *for any $\phi \in Z^2(G, A)$ there exists an extension $\mathcal{H}$ of A and a retraction r such that $\phi = \phi_{\mathcal{H},r}$;*

(c) *if r and s are two retractions of an extension $\mathcal{H}$ of A, then $\phi_{\mathcal{H},r}\phi_{\mathcal{H},s}^{-1} \in B^2(G, A)$;*

(d) *there exists a retraction which splits $\mathcal{H}$ if and only if $\phi_{\mathcal{H},r} \in B^2(G, A)$ for every retraction r.*

Proof: (a) firstly $\phi_{\mathcal{H},r}(x, y) \in A$ for every $x, y \in G$: indeed $j(r(xy)^{-1}r(x)r(y)) = (xy)^{-1}xy = 1$, so $\phi_{\mathcal{H},r}(x, y) \in \ker j = \operatorname{Im} i = A$. Moreover

$$\begin{aligned} r(xyz)\phi_{\mathcal{H},r}(xy, z)\phi_{\mathcal{H},r}(x, y)^z &= r(xyz)r(zyx)^{-1}r(xy)r(z)(r(xy)^{-1}r(x)r(y))^z \\ &= r(xy)r(z)^{-1}r(z)r(xy)^{-1}r(x)r(y)r(z) \\ &= r(x)r(y)r(z) \\ &= r(xyz)r(xyz)^{-1}r(x)r(yz)r(yz)^{-1}r(y)r(z) \\ &= r(xyz)\phi_{\mathcal{H},r}(x, yz)\phi_{\mathcal{H},r}(y, z). \end{aligned}$$

Thus $\phi_{\mathcal{H},r}(xy, z)\phi_{\mathcal{H},r}(x, y)^z = \phi_{\mathcal{H},r}(x, yz)\phi_{\mathcal{H},r}(y, z)$, that is exactly the condition for $\phi_{\mathcal{H},r} \in Z^2(G, A)$.

(b) Put $\mathcal{H} = G \times A$ (as sets) with the following operation:

$$(x, a)(y, b) = (xy, \phi(x, y)a^y b).$$

This law makes H a group with identity $(1, \phi(1, 1)^{-1})$. If we take $i : A \to H$ given by $i(a) = (1, \phi(1, 1)^{-1}a)$ and $j : H \to G$ given by $j(x, a) = x$, then i is a monomorphism, j is an epimorphism and $\ker j = \operatorname{Im} i$, so $\mathcal{H} = 1 \to A \xrightarrow{i} H \xrightarrow{j} G \to 1$ is an extension of A. If we take the retraction $r(x) = (x, 1)$, then $\phi_{\mathcal{H},r} = \phi$.

(c) Put $s(x) = r(x)\phi(x)$ for every $x \in G$, where $\phi(x) \in A$. Then

$$\begin{aligned} \phi_{\mathcal{H},s}(x, y) &= \phi(xy)^{-1}r(xy)^{-1}r(x)\phi(x)r(y)\phi(y) \\ &= \phi(xy)^{-1}r(xy)^{-1}r(x)r(y)\phi(x)^y\phi(y) \\ &= \phi(xy)^{-1}\phi_{\mathcal{H},r}(x, y)\phi(x)^y\phi(y), \end{aligned}$$

and the thesis follows by abelianity of A.

(d) If $\mathcal{H}$ is a split extension, then r is an homomorphism and then $\phi_{\mathcal{H},r}(x,y)=1$, so by (c) $\phi_{\mathcal{H},s}\in B^2$ for any other retraction s. Conversely, if for any retraction r we have $\phi_{\mathcal{H},r}(x,y)=\phi(xy)^{-1}\phi(x)^y\phi(y)\in B^2(G,A)$, then put $s(x)=r(x)\phi(x)^{-1}$; s is a retraction for $\mathcal{H}$ and we have $s(xy)=r(xy)\phi(xy)^{-1}=r(x)r(y)\phi_{\mathcal{H},r}(x,y)^{-1}\phi(xy)^{-1}=r(x)r(y)\phi(x)^{-y}\phi(xy)\phi(y)^{-1}\phi(xy)^{-1}=r(x)\phi(x)^{-1}r(y)\phi(y)^{-1}=s(x)s(y)$ and then s splits $\mathcal{H}$. $\square$

Two extensions $\mathcal{H}_1$ and $\mathcal{H}_2$ of the G-module A are *equivalent*, and we write $\mathcal{H}_1\cong\mathcal{H}_2$, if there exists an isomorphism $\sigma:H_1\to H_2$ such that the following diagram is commutative:

$$\begin{array}{lccccccc}
\mathcal{H}_1: & 1 & \longrightarrow & A & \xrightarrow{i_1} & H_1 & \xrightarrow{j_1} & G & \longrightarrow & 1\\
 & & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
\mathcal{H}_2: & 1 & \longrightarrow & A & \xrightarrow{i_2} & H_2 & \xrightarrow{j_2} & G & \longrightarrow & 1
\end{array}$$

Proposition 8 *Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be extensions of the G-module A with retractions r_1 and r_2 respectively. Put $\phi_i=\phi_{\mathcal{H}_i,r_i}$ for $i=1,2$. Then $\mathcal{H}_1\cong\mathcal{H}_2$ if and only if $\phi_1\phi_2^{-1}\in B^2(G,A)$.*

Proof: ($\Rightarrow$) Let σ be the isomorphism $H_1\to H_2$; then $\sigma(r_1(x))=r_2(x)\phi(x)$ for some $\phi(x)\in A$. Thus

$$\begin{aligned}
\phi_1(x,y) &= \sigma(\phi_1(x,y))=\sigma(r_1(xy)^{-1}r_1(x)r_1(y))\\
&= \phi(xy)^{-1}r_2(xy)^{-1}r_2(x)\phi(x)r_2(y)\phi(y)\\
&= \phi(xy)^{-1}r_2(xy)^{-1}r_2(x)r_2(y)\phi(x)^y\phi(y)\\
&= \phi_2(x,y)\phi(xy)^{-1}\phi(x)^y\phi(x).
\end{aligned}$$

($\Leftarrow$) Let $\phi_1(x,y)\phi_2(x,y)^{-1}=\phi(y)\phi(xy)^{-1}\phi(x)^y$. Put $\sigma(h_1)=r_2(x)a\phi(x)$, where $h_1=r_1(x)a\in H_1$. Then σ is the isomorphism we were looking for (easy computation). $\square$

By the two previous results it follows immediatly the following

Proposition 9 *Let A be a G-module. Then $H^2(G,A)=1$ if and only if any extension $\mathcal{H}$ of A splits.*

Now let's see a connection with the cohomology of normal subgroups. If A is a G-module and N a subgroup of G, then we can get the new structure $F_N(A)$, $T_N(A)$, $H^n(N,A)$, obtained restricting to N the domain of operation for A. Note that if N is a normal subgroup, then $F_N(A)$ is also a G/N-module by taking, for $b\in F_N(A)$ and $rN\in G/N$, $b(rN)=br$.

Proposition 10 *Let A be a G-module and $N\trianglelefteq G$. Denote $B=F_N(A)$. Then we have two exact sequences*

$$\begin{array}{ccccccccc}
H^0(N,A) & \longrightarrow & H^0(G,A) & \longrightarrow & H^0(G/N,B) & \longrightarrow & 0\\
H^1(N,A) & \longleftarrow & H^1(G,A) & \longleftarrow & H^1(G/N,B) & \longleftarrow & 0.
\end{array}$$

Proof: note that $F_G(A)=F_{G/N}(B)$ and that $T_G(A)\leqslant T_{G/N}(B)$, by $T_G(a)=T_{G/N}(T_N(a))$. So it's easy to see that the first sequence is

$$\frac{F_N(A)}{T_N(A)}\xrightarrow{T_{G/N}}\frac{F_G(A)}{T_G(A)}\xrightarrow{\pi}\frac{F_G(A)}{T_{G/N}(B)}\longrightarrow 0$$

is exact, where π is the canonical projection.
About the second one, let X be a separable G-module with A as G-submodule. Put $A^1=X/A$ and

$B^1 = F_N(X)/F_N(A)$. Then $H^1(G/N, B) \cong H^0(G/N, B^1)$, $H^1(N, A) = H^0(N, A^1)$ and $H^1(G, A) \cong H^0(G, A^1)$. One verifies that $F_{G/N}(B^1) = F_G(B^1) = (F_N(X) \cap \pi^{-1}(F_G(X/A)))/B$ and $T_{G/N}(B^1) = (B + T_{G/N}(F_N(X)))/B$, with $\pi : X \to X/A$ canonical projection. □

5.1.2 Cohomology of an irreducible G-module where G is solvable

In this paragraph suppose G finite solvable group, A multiplicative G-module such that $A^p = 1$ for some p. A is a finitely generated group and it is cyclic as G-module.

The *centralizer* of A is the set $C_G(A) = \{x \in G : ax = a \text{ for all } a \in A\}$. Note that if N is a normal subgroup of G contained in $C_G(A)$, then A can be viewed as G/N-module in a natural way; moreover any isomorphism ϕ from A to a G-module X is a G-isomorphism if and only if it is a G/N-isomorphism.

If M and N are normal subgroups of G and $M \geqslant N$, then M/N is a G-module by taking:

$$(mN)^x := x^{-1}mNx \quad \text{for } x \in G,\ m \in M;$$

certainly $C_G(M/N) \geqslant M$. Notice that M/N is a chief factor of G if and only if M/N is an irreducible G-module.

Proposition 11 *Let G be a solvable group and A an irreducible G-module. Then, if $|A| = p^r$, $G/C_G(A)$ has no proper normal p-subgroups.*

Proof: suppose there exists a normal subgroup N of G such that $C_G(A) \subset N \trianglelefteqslant G$ and $N/C_G(A)$ is a p-group. Then $F_N(A)$ is a G-submodule of A, so by irreducibility $F_N(A) = 1$ or A. $F_N(A) \neq 1$, because any orbit in A (under the action of G) has cardinality 1 or a p-power and $|F_N(A)|$ is the number of orbits of cardinality 1, so necessarly $F_N(A) > 1$ (otherwise the sum cannot be a multiple of p). Then $F_N(A) = A$ and then $N \leqslant C_G(A)$, contradiction. □

Proposition 12 *Let G be a solvable group and A an irreducible G-module. If $C_G(A) = 1$, then $H^1(G, A) = H^2(G, A) = 1$.*

Proof: if $G = 1$ the proposition is trivial, so suppose $G \neq 1$ and take $1 < N \trianglelefteqslant G$ and $(|N|, p) = 1$ (it exists by previous proposition). Then $F_N(A) = 1$, so by Prop. 7 $H^1(N, A) = 0$. Now from Prop. 10 we have the exact sequence

$$1 \quad \longrightarrow \quad H^1(G/N, F_N(A)) \quad \longrightarrow \quad H^1(G, A) \quad \longrightarrow \quad H^1(N, A),$$

that in our case becomes $1 \longrightarrow 1 \longrightarrow H^1(G, A) \longrightarrow 1$, which implies $H^1(G, A) = 1$.

In order to prove that $H^2(A) = 1$ we show that any extension of A through G splits and we conclude by Prop. 9. By Prop. 7 we have $H^1(N, A) = 1$. If H is a group such that $A \triangleleft H$ and $H/A \cong G$ and $L = \pi^{-1}(N)$ (where π is the canonical epimorphism $H \to H/A$), then by $H^2(N, A) = 1$ there exists a complement K_0 of A in L, and being $H^1(N, A) = 1$, by Theorem 4 each complement of A in L are conjugate. Now $L \triangleleft H$, so for any $h \in H$ there exists $a \in A$ such that $h^{-1}K_0h = a^{-1}K_0a$ and then, if $K = N_H(K_0)$, we have $H = KA$. Moreover $K \cap A = 1$ because A is minimal normal subgroup (it is an irreducible G-module) and being $C_G(A) = 1$. □

Corollary 2 *Let M/N be a chief factor of G solvable group. If $C_G(M/N) = M$, then M/N is complemented and all of its complements are conjugate in G.*

Proof: M/N is a simple G/M-module, so by previous proposition $H^1(G/M, M/N) = H^2(G/M, M/N) = 1$. We conclude by Theorem 4 and Prop. 9. $\square$

Now let G be a solvable group and A an irreducible G-module. Put

$$R_G(A) = \bigcap \{N \trianglelefteq G \,:\, N \leqslant C_G(A),\, C_G(A)/N \cong_G A,\, C_G(A)/N \text{ has a complement in } G/N\},$$

with $R_G(A) = C_G(A)$ if the set above is empty. Then we have $C_G(A)/R_G(A) \cong A^{\delta_G(A)}$ for a suitable integer $\delta_G(A)$ and $R_G(A)$ is minimal with this property. The number $\delta_G(A)$ is defined by the following

Proposition 13 *Let G be a solvable group, A an irreducible G-module. Then $C_G(A)/R_G(A)$ is isomorphic to the direct product of $\delta_G(A)$ copies of A, where $\delta_G(A)$ is the number of complemented chief factors of G that are G-isomorphic to A, independently on the choice of the chief series.*

Proof: if A is not isomorphic to any chief factor of G, $R_G(A) = C_G(A)$ and the statement is trivial.

Now let $\mathcal{L}$ be the chief series $G = G_r > \cdots > G_1 > G_0 = 1$, with $C_G(A) \in \mathcal{L}$ and let m be the number of complemented chief factors of $\mathcal{L}$ G-isomorphic to A. We distinguish two cases:

(a) suppose G_1 is not complemented or it is not G-isomorphic to A. Then $R_G(A) \geqslant G_1$, otherwise there would be $N \trianglelefteq G$ such that $N \leqslant C_G(A)$ and $C_G(A)/N \cong_G A$: thus $G_1 \cong_G A$ and by Corollary 2 there would exist a complement K/N of $C_G(A)/N$ in G/N and K would be a complement of G_1 in G, contradicion.

Now m is the number of complemented chief factor G/G_1-isomorphic to A, i.e G-isomorphic to A in the chief series of G/G_1 induced by $\mathcal{L}$; by induction on the length of $\mathcal{L}$ we get $m = \delta_{G/G_1}(A)$. By $G_1 \leqslant R_G(A)$, we get

$$\frac{C_{G/G_1}(A)}{R_{G/G_1}(A)} \cong_{G/G_1} \frac{C_G(A)}{R_G(A)} \Rightarrow \frac{C_{G/G_1}(A)}{R_{G/G_1}(A)} \cong_G \frac{C_G(A)}{R_G(A)},$$

and then $m = \delta_G(A)$.

(b) Suppose G_1 is G-isomorphic to A and complemented in G: say K its complement. Put $\overline{R}/G_1 = R_{G/G_1}(A)$. Then $C_G(A)/(K \cap C_G(A)) \cong_G G_1 \cong_G A$. By definition of $R_G(A)$ we have $R_G(A) \leqslant \overline{R} \cap K$. If it would be $R_G(A) < \overline{R} \cap K$, then also $R_G(A)G_1 < \overline{R}$ and $C_{G/G_1}(A)/(\overline{R}/G_1)$ would be semisimple, against the definition of $R_{G/G_1}(A)$. Then $\overline{R} \cap K = R_G(A)$ and $\delta_G(A) - 1 = \delta_{G/G_1}(A)$. The number of complemented chief factors G-isomorphic to A in the chief series of G/G_1 induced by $\mathcal{L}$ is $m - 1$, so we can proceed by induction and get the thesis. $\square$

Proposition 14 *$C_G(A)/R_G(A)$ is complemented in $G/R_G(A)$.*

Proof: by Prop. 12 we have $H^2(G/C_G(A), A) = 1$. Thus $H^2(G/C_G(A), A^{\delta_G(A)}) = 1$ and we conclude by Prop. 9 bearing in mind that $C_G(A)/R_G(A) \cong_G A^{\delta_G(A)}$. $\square$

Theorem 6 *Let G be a solvable group and A an irreducible G-module. Then $H^1(G, A) \cong \mathrm{End}_G(A)^{\delta_G(A)}$.*

Proof: for convenience write $C = C_G(A)$ and $R = R_G(A)$.

Let $\phi \in Z^1(G, A)$ and $\overline{\phi}$ its restriction to C; then the application $\tau : \phi \mapsto \overline{\phi}$ induces an homomorphism from $Z^1(G, A)$ to $\mathrm{Hom}_G(C/R, A)$: for any $x, y \in C$ we have $\phi(xy) = \phi(xy) = \phi(x)^y\phi(x) = \phi(x)\phi(y)$ and if $g \in G$ we have $\phi(g^{-1}xg) = \phi(g^{-1})^{xg}\phi(x)^g\phi(g) = \phi(g^{-1})^g\phi(x)^g\phi(g) = \phi(x)^g$; being $\phi(g^{-1})^g\phi(g) = \phi(1) = 1$ and $\overline{\phi}$ is trivial on R, i.e. $\ker\tau$ contains R.

Now let $\gamma \in \mathrm{Hom}_G(C/R, A)$ and suppose by Prop. 14 that there exists $K \leqslant G$ such that $G = KC$ and $K \cap C = R$. Put $\phi(x) = \gamma(cR)$, where $x = kc$ for $k \in K$ and $c \in C$. Then ϕ is well-defined

and certainly $\overline{\phi} = \gamma$. Let's verify that $\phi \in Z^1(G, A)$: if $x, y \in G$, $x = kc$, $y = ld$ (with $k, l \in K$ and $c, d \in C$), then $\phi(xy) = \phi(kcld) = \phi(kll^{-1}cld) = \gamma(l^{-1}cldR) = \gamma(cR)^l\gamma(dR)$. On the other hand $\phi(x)^y\phi(x) = \gamma(cR)^{ld}\gamma(dr) = \gamma(cR)^l\gamma(dR)$, as we wished.

Finally verify that $\phi \in B^1(G, A)$ if and only if $\overline{\phi} = 1$. $\phi \in B^1(G, A)$ implies $\varphi^x\varphi^{-1}$ for some $\varphi \in A$; then $\phi(x) = 1$ if $x \in C$. Conversely if $\overline{\phi} = 1$, then ϕ is constant on any xC, $x \in G$ and then the function ψ defined by $\psi(xC) = \phi(x)$ is well-defined on G/C and $\psi \in Z^1(G/C, A)$. By Prop. 12 we have $\psi \in B^1(G/C, A)$ and then for $xC \in G/C$, $\psi(xC) = \varphi^{xC}\varphi^{-1}$ with $\varphi \in A$, that is $\phi(x) = \varphi^x\varphi^{-1}$ for every $x \in G$; then $\phi \in B^1(G, A)$.

In conclusion we have the exact sequence

$$1 \longrightarrow B^1(G, A) \longrightarrow Z^1(G, A) \longrightarrow \mathrm{Hom}_G(C/R, A) \longrightarrow 1$$

and it follows $H^1(G, A) \cong \mathrm{Hom}_G(C/R, A) \cong \mathrm{Hom}_G(A^{\delta_G(A)}, A) \cong \mathrm{End}_G(A)^{\delta_G(A)}$. □

5.1.3 Number of generators and Eulerian function of a solvable group

Let G be a (arbitrary) group. The *eulerian function* of G is the function ϕ_G from $\mathbb{N}$ in the set of cardinals defined by

$$\phi_G(k) = \left|\{(x_1, \ldots, x_k) \in G^k \,:\, \langle x_1, \ldots, x_k\rangle = G\}\right|.$$

For example: if $G = \mathbb{Z}_n$ cyclic group of order n, then $\phi_G(1) = \phi(n)$ the classical Euler function.

Proposition 15 *Let G be a group and M an abelian minimal normal subgroup of G and write $G/M = \langle \overline{x}_1 M, \ldots, \overline{x}_k M\rangle$. If $c(M)$ is the number of complements of M in G, then there are exactly $|M|^k - c(M)$ k-tuples $(x_1, \ldots, x_k)$ such that $x_i \in \overline{x}_i M$ and $\langle x_1, \ldots, x_k\rangle = G$.*

Proof: the number of k-tuples $(x_1, \ldots, x_k)$ with $x_i \in \overline{x}_i M$ is clearly $|M|^k$. Now either$\langle x_1, \ldots, x_k\rangle = G$ or it is a complement of M in G. But for any complement K of M in G it is uniquely determined the k-tuple $x_i = \overline{x}_i M \cap K$. □

Corollary 3 *Let G be a group and M an abelian minimal normal subgroup of G. Then*

$$\phi_G(k) = \phi_{G/M}(k)(|M|^k - c(M)).$$

Proof: if $\langle \overline{x}_1, \ldots, \overline{x}_k\rangle = G$, then $\langle \overline{x}_1 M, \ldots, \overline{x}_k M\rangle = G/M$. The result follows directly by Prop. 15. □

Proposition 16 *Let G be a solvable group, M an abelian minimal normal subgroup of G. If M is complemented, then*

$$c(M) = |\mathrm{End}_G(A)|^{\delta_G(A)-1}|A|^{\theta_G(A)},$$

where $A \cong_G M$ as G-module and $\theta_G(A) = 0$ or 1 according as A is the trivial G-module or not.

Proof: let K be a complement of M in G. K is maximal in G. The number of conjugates of K in G is equal to $|G : N_G(K)| = 1$ or $|A|$ according as M is in the center of G or not. By Theorem 4 the number of conjugacy classes of complements of M in G is $|H^1(G/M, A)|$, and by Prop. 13 and Theorem 6 $|H^1(G/M, A)| = |\mathrm{End}_G(A)|^{\delta_G(A)-1}$. □

Theorem 7 *Let G be a solvable group, then:*

$$\phi_G(k) = \frac{|G|^k}{\left(\prod_A |A|^{\delta_G(A)}\right)^k} \prod_A \left(\prod_{i=0}^{\delta_G(A)-1} |A|^k - |\mathrm{End}_G(A)|^i |A|^{\theta_G(A)} \right), \tag{5}$$

where A runs over all complemented chief factors of G.

Proof: we work by induction on the length of a chief series $G = G_r > \cdots > G_1 > G_0 = 1$ of G.

Let $G_1 \cong A$ and suppose the formula holds for G/G_1. By Corollary 3 $\phi_G(k) = \phi_{G/G_1}(k)(|G_1|^k - c(A))$. If $k = 0$, then

$$\phi_G(k) = \phi_{G/G_1}(k)|G_1|^k = \phi_{G/G_1}(k)\frac{|G|^k}{|G/C_1|^k}.$$

If $k \neq 0$, then by Prop. 16 $c(A) = |\mathrm{End}_G(A)|^{\delta_G(A)-1}|A|^{\theta_G(A)}$ and then

$$\phi_G(k) = \phi_{G/G_1}(k)(|A|^k - |\mathrm{End}_G(A)|^{\delta_G(A)-1}|A|^{\theta_G(A)}). \qquad \square$$

Now it's clear that $P_G(k) = \phi_G(k)/|G|^k$, so dividing the formula 5 by $|G|^k$ we get

$$P_G(k) = \prod_A \left(\prod_{i=0}^{\delta_G(A)-1} 1 - \frac{|\mathrm{End}_G(A)|^i |A|^{\theta_G(A)}}{|A|^k} \right).$$

5.2 The formula in the profinite case

Now we need some work to generalize these arguments to the profinite case.
We say that H/K is a *chief factor* of G if H and K are closed normal subgroups of G with $K < H$ and there are no intermediate closed normal subgroups (i.e. if X is a closed normal subgroup of G such that $K \leqslant X \leqslant H$, then either $X = H$ or $X = K$). We are interested to the case of prosupersolvable groups, so any chief factor is cyclic and then abelian. Since $X = \bigcap\{XN,\ N \trianglelefteqslant G \text{ open}\}$ for every closed subset X, necessarly $HN \neq KN$ for at least one open normal subgroup N, and so $H/K \cong_G HN/KN$. This implies that H/K is finite and the action of G on H/K is continuous and irreducible.

A chief factor H/K is called *Frattini factor* if $H/K \leqslant \mathrm{Frat}(G/K)$. Notice that if H/K is a Frattini factor, so is HN/KN for every $N \trianglelefteqslant G$ closed. Now let's give a definition.

Let A be a finite irreducible G-group with G prosolvable. Let $\mathcal{X}_G(A)$ be the set of the open normal subgroups N of G with the properties that $N \leqslant C_G(A)$, $C_G(A)/N \cong_G A$ and $C_G(A)/N$ is non-Frattini, and define

$$R_G(A) = \bigcap_{N \in \mathcal{X}_G(A)} N$$

and $R_G(A) = C_G(A)$ if $\mathcal{X}_G(A)$ is empty. The quotient group $C_G(A)/R_G(A)$ is called the *A-crown* of G.

Note that two G-isomorphic G-groups define the same crown. Since $R_G(A)$ and $C_G(A)$ are closed normal subgroups of G, then the quotient groups $G/R_G(A)$ and $C_G(A)/R_G(A)$ are profinite groups

with a fundamental system of neighborhoods given by the family of subgroup $N/R_G(A)$ where N is a finite intersection of elements of $\mathcal{X}_G(A)$.

We want to study the structure of $G/R_G(A)$. First note that $R_G(A) \neq C_G(A)$ if and only if A is equivalent to a non-Frattini chief factor of G; so we restrict out attention to this case. Moreover, since we are dealing with prosupersolvable groups, we assume that A is abelian.

Define the *monolithic primitive group associated with* A the group

$$L_G(A) = A \rtimes (G/C_G(A)).$$

Simplify our notation by identifying $C = C_G(A)$, $R = R_G(A)$, $L = L_G(A)$ and $\mathcal{X} = \mathcal{X}_G(A)$ and let $\mathcal{Y}$ be the set of all normal subgroups of G obtained as finite intersections of elements in $\mathcal{X}$; we remark that G/R is the inverse limit of the family of finite groups G/N with $N \in \mathcal{Y}$.

Now we want to describe the structure of G/R. Define the *crown-based power* of L of size k the group

$$L_k = \{(l_1, \dots, l_k) \in L^k \,:\, l_1 \equiv \cdots \equiv l_k \pmod{A}\} = A^k \rtimes (G/C_G(A)).$$

Now we have the following results.

Lemma 2 *Let $Y \in \mathcal{Y}$, $Y = N_1 \cap \cdots \cap N_k$ with k minimal. Then $G/Y \cong L_k$. Moreover $C/Y = \mathrm{soc}(G/Y)$ and any chief factor H/K of G with $Y \leqslant K < H \leqslant C$ is non-Frattini and G-isomorphic to A.*

Proof: the Lemma follows by the following result in finite case (see Prop. 9, [2]): let A be a non-Frattini chief factor of the finite group G and $C_G(A)/R_G(A)$ its crown. Then $G/R_G(A)$ is isomorphic to $L_{\delta_G(A)}(A)$, with $\delta_G(A) < \infty$ since G is finitely generated. By Prop. 13 $C_G(A)/R_G(A) \cong_G A^{\delta_G(A)}$, and by $R_G(A) \leq Y \leq C_G(A)$, it follows $Y \cong_G A^u$ for some $u \leq \delta_G(A)$. Then $G/Y \cong_G L_{\delta_G(A)-u}$. $\square$

Corollary 4 *If N is a closed normal subgroup of G and $R \leqslant N$ then either $C \leqslant N$ or $N \leqslant C$. Moreover if N is open and $R \leqslant N < C$, then $N \in \mathcal{Y}$.*

Proof: as N is closed and $\{Y/R\}_{Y \in \mathcal{Y}}$ is a fundamental system of open neighborhoods of the identity in G/R, then $N = \bigcap_{Y \in \mathcal{Y}} NY$. Now NY/Y is a normal subgroup of the finite group G/Y which is isomorphic to L_k for some k by previous lemma. It follows that $C/Y = \mathrm{soc}(G/Y)$ and also either $NY \leqslant C$ or $NY > C$. In the first case we conclude $N \leqslant C$. Otherwise $NY > C$ for every $Y \in \mathcal{Y}$, and thus $N = \bigcap_{Y \in \mathcal{Y}} NY \geqslant 1$. $\square$

We can define crown-based power of L of infinite rank too in the following way: for any set Ω take

$$L_\Omega = \{(l_\omega)_{\omega \in \Omega} \in L^\Omega \,:\, l_{\omega_1} \equiv l_{\omega_2} \pmod{A} \text{ for any } \omega_1, \omega_2 \in \Omega\}.$$

It is a closed subgroup of L^Ω with the product topology, so it can be viewed as a profinite group: indeed L_Ω is the inverse limit of the family of finite groups L_I with $I \subseteq \Omega$ finite.

Let now $\mathcal{D}$ be the set of subsets Δ of $\mathrm{Hom}(G, L)$ satisfying:

(1) for any $\phi \in \Delta$, $\ker \phi \in \mathcal{X}$;

(2) for any finite subset $I = \{\phi_1, \dots, \phi_k\}$ of Δ and $g \in G$ we have $\phi_1(g) \equiv \cdots \equiv \phi_k(g) \pmod{A}$, i.e. they define an homomorphism $\phi_I : G \to L_k$;

(3) for any finite subset $I \subseteq \Delta$, the homomorphism ϕ_I is surjective.

This definition implies that if $\Delta \in \mathcal{D}$, then the functions ϕ_I are compactible surjections from G to $\varprojlim L_I$; thus the corresponding induced mapping of profinite groups $\Phi : G \to L_\Delta$ is onto. Moreover $\ker \phi_I \in \mathcal{Y}$ and so $\ker \Phi = \bigcap_{\phi\in\Delta} \ker \phi$ is an intersection of elements of $\mathcal{X}$.

We may order the elements of $\mathcal{D}$ by inclusion, and by Zorn's Lemma $\mathcal{D}$ has a maximal element.

Lemma 3 *If Δ is a maximal element of $\mathcal{D}$, then $\bigcap_{\phi\in\Delta} \ker \phi = R$.*

Proof: for any $\phi \in \Delta$, let $N_\phi = \ker \phi \in \mathcal{X}$. Suppose by contradiction $S = \bigcap_{\phi\in\Delta} N_\phi \neq R$. Then there exists $N \in \mathcal{X}$ with $S \not\leqslant N$ and an epimorphism $\alpha : G \to L$ with $\ker \alpha = N$. Fix $\bar\phi \in \Delta$; the map $G/(N_{\bar\phi} \cap N) \to L^2$ defined by $g(N_{\bar\phi} \cap N) \mapsto (\bar\phi(g), \alpha(g))$ is injective; by Lemma 2 $G/(N_{\bar\phi} \cap N) \cong L_2$, hence there exists $\beta \in \mathrm{Aut}(L)$ such that $\beta^{-1}\alpha(g)\beta \cong \bar\phi(g) \pmod{\mathrm{soc}(L)}$ for any $g \in G$. Let $\gamma : G \to L$ be defined by $\gamma(g) = \alpha(g)^\beta$. Now let $\bar\Delta = \Delta \cup \{\gamma\}$. We claim that $\bar\Delta \in \mathcal{D}$, against the maximality of Δ. The only thing that remains to prove is that for any finite subset $I = \{\phi_1, \ldots, \phi_k\}$ of Δ, the homomorphism $\bar\phi_I : G \to L_{k+1}$ defined by $g \mapsto (\phi_1(g), \ldots, \phi_k(g), \gamma(g))$ is surjective. By Lemma 5 and the fact that ϕ_I is surjective, either $\bar\phi_I$ is surjective or $G/(N_{\phi_1} \cap \cdots \cap N_{\phi_k}) \cong G/(N_{\phi_1} \cap \cdots \cap N_{\phi_k} \cap N) \cong L_k$. But in the latter case $S \leqslant N_{\phi_1} \cap \cdots \cap N_{\phi_k} \leqslant N$, a contradiction. □

Let $w_0(G)$ denote the local weight of the profinite group G, i.e. the smallest cardinality of a fundamental system of open neighborhoods of 1 in G. Then

Theorem 8 *G/R is homeomorphic to L_Ω, for a suitable choice of the set Ω. If $\mathcal{X}$ is infinite, then $|\Omega| = |\mathcal{X}|$.*

Proof: by previous lemma G/R is homeomorphic to L_Ω, where Ω is a maximal element of $\mathcal{D}$. Since a base of neighborhoods of 1 in G/R is given by the subgroups N/R for $N \in \mathcal{Y}$, if $\mathcal{X}$ is infinite then $|\mathcal{X}| = |\mathcal{Y}| = w_0(G/R)$. On the other hand, $w_0(G/R) = w_0(L_\Omega)$ is the cardinality of the set of the finite subsets of Ω, which is exactly the cardinality of Ω for Ω infinite. □

Recall that any profinite group G has a chain of closed normal subgroups

$$1 = G_\mu \lhd \cdots \lhd G_\lambda \lhd \cdots \lhd G_0 = G$$

indexed by 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 $G_\lambda = \bigcap_{\nu\leq\lambda} G_\nu$.

Note that if G is infinite, then $|\mu| = w_0(G)$, so $|\mu|$ is an invariant.

In our case G is a prosupersolvable group, so $G_\lambda/G_{\lambda+1}$ is cyclic for every $\lambda < \mu$.

Lemma 4 *Let H/K be a chief factor of G. If $R \leqslant K < H \leqslant C$ then H/K is non-Frattini and G-isomorphic to A.*

Proof: since $\mathcal{Y}$ induces a fundamental system of open neighborhoods of the identity in C/R, we get $K = \bigcap_{N\in\mathcal{Y}} KN$ and $H = \bigcap_{N\in\mathcal{Y}} HN$. Thus there exists $N \in \mathcal{Y}$ such that $KN \neq HN$ and so $H/K \cong_G HN/KN$. By Lemma 2 HN/KN is non-Frattini and G-isomorphic to A, and thus the same holds for H/K. □

Lemma 5 *Let H/K be a chief factor of G. Then H/K is non-Frattini and G-isomorphic to A if and only if $RH/RK \neq 1$ and $RH \leqslant C$.*

Proof: if $RK \neq RH \leqslant C$, then by Lemma 4, RH/RK is non-Frattini and G-equivalent to A. As $H/K \not\leqslant \mathrm{Frat}(G/K)$, there exists a closed maximal subgroup M containing K but not H. Let $N = M_G$ be the normal core; since H and K are normal in G, we deduce $K \leqslant N$ and $H \not\leqslant N$. In particular HN/N is a minimal normal subgroup of the primitive group G/N and it is G-isomorphic to H/K, hence to A. Note that, C/N is the socle of G/N. Then either $C/N = HN/N$ and $N \in \mathcal{X}$ or $N \in \mathcal{Y}$ (see Lemma 3, [3]). In particular $R \leqslant N = NK < NH \leqslant C$ and so $RK \neq RH \leqslant C$. □

The following theorem proves the result just known in the finite case.

Theorem 9 *Let $\{G_\lambda\}_{\lambda\leq\mu}$ be a chief series of G and let Θ be the set of factors $G_\lambda/G_{\lambda+1}$ which are non-Frattini and G-isomorphic to A. The cardinality $\delta_G(A)$ of Θ does not depend on the choice of the chief series. Moreover if $G/R \cong L_\Omega$ then $|\Omega| = \delta_G(A)$.*

Proof: we obtain a chain of closed normal subgroups $\{H_\lambda\}_{\lambda\leq\mu}$ with $H_0 = G$ and $H_\mu = R$ by defining $H_\lambda = RG_\lambda$. For any $\lambda \leq \mu$, either $H_\lambda = H_{\lambda+1}$ or $H_\lambda/H_{\lambda+1}$ is a chief factor of G/R. Moreover the set of non trivial factors $H_\lambda/H_{\lambda+1}$ coincides with the set of factors of a chief series of G/R. By Corollary 4 either $H_\lambda \leq C$ or $H_\lambda \geq C$. Let ν be the smallest ordinal with $H_\nu \leq C$. Now Lemma 5 implies that if $\lambda < \nu$, $G_\lambda/G_{\lambda+1}$ cannot be non-Frattini and G-isomorphic to A; moreover, if $\lambda \geq \nu$, then $H_\lambda/H_{\lambda+1} \neq 1$ if and only if $G_\lambda/G_{\lambda+1}$ is non-Frattini and G-isomorphic to A.

So $\{H_\lambda/H_{\lambda+1} : H_\lambda/H_{\lambda+1} \neq 1\}$ is a chief series of G/R which passes through C/R and has the property that the elements of Θ are in bijective correspondence with the non trivial factors $H_\lambda/H_{\lambda+1}$ contained in C/R; in particular $|\Theta|$ does not depend on the choice of the series.

Finally, since $G/R \cong L_\Omega$ implies $C/R \cong A^\Omega$, we conclude $|\Theta| = |\Omega|$. □

Theorem 10 *If G is finitely generated then $\delta_G(A)$ is finite for every finite irreducible G-group A.*

Proof: if $X \in \mathcal{X}_G(A)$, then by definition $C/X \cong A$ and then $|G : X| = |G : C||A| = n$ for an integer n. As G is finitely generated, the number of subgroups of index n is finite; thus $|\mathcal{X}_G(A)|$ is finite and consequently R has finite index in G. Therefore $G/R \cong L_\Omega$ for a finite set Ω and the result follows from the previous theorem. □

Now we have, for a profinite group G, the formula

$$P_G(k) = \sum_{H\leqslant G} \frac{\mu(H)}{|G : H|^k}, \tag{6}$$

where μ is the Möbius function of the subgroup lattice of G. If G is finite, then $P_G(k)$ is a finite Dirichlet series $\sum_n a_n n^{-k}$, with $a_n \in \mathbb{Z}$ and $a_n = 0$ unless n divides $|G|$. So the formula can be extended to an arbitrary complex number s. Given a normal subgroup N of G, we defined the formal Dirichlet series $P_{G,N}(s)$ as follows:

$$P_{G,N}(s) = \sum_{HN=G} \frac{\mu(H)}{|G : H|^s}. \tag{7}$$

We can write the two formal Dirichlet series as follows:

$$P_G(s) := \sum_{n>0} \frac{a_n}{n^s} \qquad \text{with } a_n := \sum_{|G:H|=n} \mu(H), \tag{8}$$

and

$$P_{G,N}(s) := \sum_{n>0} \frac{b_n}{n^s} \qquad \text{with } b_n := \sum_{\substack{|G:H|=n,\\ HN=G}} \mu(H). \tag{9}$$

If $A(s)$ and $B(s)$ are two Dirichlet series, denote with $A(s) * B(s)$ the convolution product of A and B. Then we have:

Theorem 11 *If G is a 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: we have already seen the result in the finite case, so we need an argument to reduce us to the finite case. Let $n \in \mathbb{N}$. The coefficients of $1/n^s$ in $P_G(s)$ and in $P_{G/N}(s) * P_{G,N}(s)$ are equal if

$$\sum_{|G:H|=n} \mu(H) = \sum_{d|n} \left(\left(\sum_{\substack{N \leqslant H_1 \leqslant G \\ |G:H_1|=d}} \mu(H_1) \right) \left(\sum_{\substack{H_2 N = G \\ |G:H_2|=n/d}} \mu(H_2) \right) \right). \tag{10}$$

Let X_n be the intersection of the open subgroups of G with index at most n; as G is finitely generated, X_n has finite index in G. Thus

$$P_{G/X_n}(s) = P_{G/NX_n}(s) * P_{G/X_n, NX_n/N_n}(s). \tag{11}$$

Now (10) follows by (11) since the terms in (10) are equal to the coefficients of $1/n^s$ in the two series in (11); indeed if $|G : H| \leq n$, then $X_n \leqslant H$ and $\mu(H) = \mu(H/X_n)$. $\square$

In the case of a finite group G, if we take a chief series

$$\sigma : 1 = N_l \lhd N_{l-1} \lhd \cdots \lhd N_1 \lhd N_0 = G$$

and iterate the above formula, we get an expression for $P_G(s)$ as product indexed by the non-Frattini chief factors in the series

$$P_G(s) = \prod_{N_i/N_{i+1} \not\leqslant \mathrm{Frat}(G/N_{i+1})} P_{G/N_{i+1}, N_i/N_{i+1}}(s). \tag{12}$$

We have just proved that the formula can be rewritten as

$$P_G(s) = \prod_A \left(\prod_{0 \leq i \leq \delta_G(A)-1} \widetilde{P}_{L_A,i}(s) \right),$$

with $\widetilde{P}_{L_A,i}(s) = 1 - |\mathrm{End}_G(A)|^i |A|^{\theta_G(A)} / |A|^s$ and A runs over all non-Frattini chief factors of G. We want to show that this formula yields in the case G prosolvable too (in this case the first product will be infinite).

Theorem 12 *Let G be a finitely generated prosolvable group and let $A = H/K$ be a non-Frattini chief factor of G. If $R = R_G(A)$ we have:*

$$P_{G/K,H/K}(s) = P_{G/RK,RH/RK}(s) = \widetilde{P}_{L_A,k}(s)$$

with $k = \delta_G(A)$.

Proof: take $\mathcal{S}_n = \{X \leqslant G : K \leqslant X \leqslant G, XH = G, |G : X| = n \text{ and } \mu(X) \neq 0\}$; $P_{G/K,H/K}(s) = \sum_n \alpha_n/n^s$ with $\alpha_n = \sum_{X\in\mathcal{S}_n} \mu(X)$. Now $\mu(X) \neq 0$ only if X is intersection of closed maximal subgroups of G. Moreover in the proof of Lemma 5 we have seen that if M is a closed maximal subgroup of G with $K \leqslant M$ but $H \not\leqslant M$, then $R \leqslant M$; hence $RK \leqslant X$ for any $X \in \mathcal{S}_n$. This implies immediatly that $P_{G/K,H/K}(s) = P_{G/RK,RH/RK}(s)$.

Now by Theorems 9 and 10 we get that $k = \delta_G(A)$ is finite and $G/RK \cong L_k$. Moreover RH/RK is a minimal normal subgroup of G/RK that is equivalent to A. By the finite case we conclude $P_{G/RK,RH/RK}(s) = \widetilde{P}_{L_A,k}(s)$. $\square$

If G is an infinite finitely generated profinite group, then $w_0(G) = \aleph_0$ and G has a chief series of length $\aleph_0$

$$\Sigma : G = G_0 > G_1 > \cdots > G_i > \cdots > G_{\aleph_0} = 1.$$

To each chief factor G_i/G_{i+1} is associated the finite Dirichlet series $P_{G/G_{i+1},G_i/G_{i+1}}(s)$. By Theorem 12, for any $i \in \mathbb{N}$, we can write

$$P_{G/G_{i+1}}(s) = P_0(s) * P_1(s) * \cdots * P_i(s).$$

So we are tempted to say that $P_G(s)$ is the product of the infinite factors $\{P_i(s)\}_{i\in\mathbb{N}}$.
Unfortunately the formal series $P_G(s)$ is not necessarly convergent, so $P_G(s)$ does not define a function in general. However it can be proved (see [3]) that the formal Dirichlet series $P_G(s)$ is uniquely determined as an "infinite convolution" of the factors $\{P_i(s)\}_{i\in\mathbb{N}}$ and that the set of factors is independent on the choice of the chief series Σ. In our case we have a prosolvable group and we are interested to the case $s = t$ integer. In the first section we saw that the product converges for t large enough.

5.3 The free prosupersolvable case and its convergence

In order to get information about the convergence of our formula for supersolvable groups it is sufficient to consider the free prosupersolvable group of rank d. In fact, any supersolvable group H of rank d is epimorphic image of G, so the chief series of H is a "subset" of the chief series of G and then the Dirichlet product for $P_H(s)$ will be composed just by some of the factors of the Dirichlet product for $P_G(s)$.

In the prosupersolvable group G any chief factor is cyclic of prime order p, so the formula can be rewritten in the form

$$P_G(s) = \prod_p \left(\prod_{|A|=p} \left(\prod_{i=0}^{\delta_G(A)-1} 1 - \frac{|\mathrm{End}_G(A)|^i |A|^{\theta_G(A)}}{|A|^s} \right) \right).$$

We need to know how many non-complemented chief factor of order p pairwise non-G-isomorphic are there and, for each of these, to estimate the value of $\delta_G(A)$.

Firstly A is the cyclic group of order p, so $\mathrm{End}_G(A) \cong C_p$.
A nontrivial action of G over A is identified by a homomorphism $\varphi : G \to \mathrm{Aut}(A) \cong \mathrm{Aut}(C_p) \cong C_{p-1}$. Any generator of G can be sent in any element of C_{p-1}, so there are $(p-1)^d$ choices for φ. We are sure that two modules obtained by two different homomorphisms φ_1 and φ_2 are not G-isomorphic. Indeed in this case we should have an automorphism $\alpha \in \mathrm{Aut}(C_p)$ such that $\alpha(\varphi_1(g)(x)) = \varphi_2(g)(\alpha(x))$ for every $x \in A$ and $g \in G$. This implies $\varphi_1(g)\alpha = \alpha\varphi_2(g)$ and then $\varphi_1 = \varphi_2$ because C_{p-1} is abelian.

It remains to estimate $\delta_G(A)$. Let's consider the A-crown $L_t = A^t \rtimes H$ of rank t, with $H = G/C_G(A)$. L_t is finite supersolvable (it's easy to find a chief series of cyclic groups), and it is $(t+\theta_G(A))$-generated, because $H = 1$ if A is the trivial G-module, otherwise it is cyclic being A cyclic of prime order. Then L_t is epimorphic image of the free prosupersolvable group G of rank d if and only if $t + \theta_G(A) \leq d$, i.e. $t \leq d - \theta_G(A)$. On the other hand, by Theorem 9 L_t is epimorphic image of G if and only if $t \leq \delta_G(A)$. By this two observations we have $\delta_G(A) = d - \theta_G(A)$.

So the formula becomes:

$$\begin{aligned} P_G(s) &= \prod_p \left(\prod_{|A|=p} \left(\prod_{i=0}^{\delta_G(A)-1} 1 - \frac{|\mathrm{End}_G(A)|^i |A|^{\theta_G(A)}}{|A|^s} \right) \right) \\ &= \prod_p \left[\left(\prod_{i=0}^{d-2} 1 - \frac{p^{i+1}}{p^s} \right)^{\alpha_p} \left(\prod_{i=0}^{d-1} 1 - \frac{p^i}{p^s} \right) \right] \\ &= \prod_p \left[\left(\prod_{i=1}^{d-1} 1 - \frac{p^i}{p^s} \right)^{\alpha_p} \left(\prod_{i=0}^{d-1} 1 - \frac{p^i}{p^s} \right) \right], \end{aligned}$$

where $\alpha_p = (p-1)^d - 1$; the first term involves all non-trivial G-submodules A of order p and the second term regards the trivial G-submodule A.

We are looking for the minimum integer k such that $P_G(k) > 0$. Since the product $\prod(1 + x_n)$ converges if and only if the sum $\sum x_n$ converges, then $P_G(k)$ converges if and only if converges the sum

$$\sum_p \left(\sum_{i=1}^{d-1} ((p-1)^d - 1) \frac{p^i}{p^k} + \sum_{i=0}^{d-1} \frac{p^i}{p^k} \right) \sim \sum_p \left(\frac{p^d - 1}{p-1} \right) \frac{p^d}{p^k} \sim \sum_p \frac{p^{2d-1}}{p^k},$$

that converges if $k - (2d-1) > 1$.

In conclusion $P_G(k) > 0$ for $k > 2d$, so we may expect to generate G with positive probability with $k \geq 2d + 1$ elements.

References

[1] A. Mann, Positively finitely generated groups. *Forum Math.* 8 (1996), no. 4, 429–459.

[2] E. Detomi; A. Lucchini. Crowns and factorization of the probabilistic zeta function of a finite group. *J. Algebra* 265 (2003), no. 2, 651–668.

[3] Detomi, Eloisa; Lucchini, Andrea. Crowns in profinite groups and applications. *Noncommutative algebra and geometry*, 47–62, Lect. Notes Pure Appl. Math., 243, *Chapman and Hall/CRC, Boca Raton, FL*, 2006.

[4] A. Lucchini; F. Menegazzo; M. Morigi. On the probability of generating prosoluble groups. *Israel J. Math.* 155 (2006), 93–115.

[5] John S. Wilson, *Profinite groups*, (1998), 68-72

[6] P. Förster, Chief factors, crowns, and the generalised Jordan-Hölder theorem. *Comm. Algebra* 16 (1988), no. 8, 1627–1638.

[7] B. C. Oltikar, L. Ribes, On prosupersolvable groups. *Pacific J. Math.* 77 (1978), no. 1, 183–188.

[8] A. Fort. Lezioni sulla coomologia dei gruppi finiti, *Programma professori visitatori* (1973) 9-30, 58-67

[9] N. Boston. A probabilistic generalization of the Riemann zeta function. *Analytic number theory*, Vol. 1 (Allerton Park, IL, 1995), 155–162, Progr. Math., 138, *Birkhäuser Boston, Boston, MA*, 1996.

[10] P. Hall. The Eulerian functions of a group, *Quart. J. Math.* 7 (1936), 134-151

[11] I. Pak. On the probability of generating a finite group, *Preprint* (2000)

[12] P. Jiménez-Seral; J. P. Lafuente. On complemented nonabelian chief factors of a finite group. *Israel J. Math.* 106 (1998), 177–188.

[13] T. Weigel. On the probabilistic zeta-function of pro(finite-soluble) groups. *Forum Math.* 17 (2005), no. 4, 669–698.

[14] M. Morigi. On the probability of generating free prosoluble groups of small rank. *Israel J. Math.* 155 (2006), 117–123.

[15] A. Lucchini. Subgroups of solvable groups with non-zero Möbius function. *J. Group Theory* 10 (2007), no. 5, 633–639.