Università degli Studi di Padova

Dipartimento di Matematica

Corso di Laurea Magistrale in Matematica

Intersections of Maximal Subgroups in Finite Solvable Groups

Laureando:
Iker de las Heras

Relatore:
Dott. Andrea Lucchini

Anno accademico 2016/2017

Contents

Introduction

Let G be a finitely generated profinite group (in topological groups finitely generated will always mean topologically finitely generated). Since it is finitely generated, there is a finite number of subgroups of any given index, and we write $c_n(G)$ to express the number of subgroups of G of index n which are intersections of (open) maximal subgroups. We will say that $c_n(G)$ is polynomially bounded if there exists β independent of n such that $c_n(G) \leq n^{\beta}$. In [13], Mann makes the following question.

Problem 1. What are the groups for which $c_n(G)$ is polynomially bounded?

Let us see what brought Mann to ask this question (all notions and almost all the results in this introduction will be analysed in detail in Chapter 1). Let $P_G(t)$ be the probability that t random elements of G generate G, and let μ_G be the Möbius function of G defined for all finite index subgroups of G by the rules: $\mu_G(G) = 1$ and $\mu_G(H) = -\sum_{K>H} \mu_G(K)$ for $H < G$. In [7], Hall proved that for finite groups we have

$$P_G(t) = \sum_{H \leq G} \mu_G(H)/|G : H|^t. \tag{1}$$

Thus, in [13], Mann tries to get a generalization for finitely generated profinite groups, wondering if this sum also holds for them. He proves that if G is prosolvable, then (1) is convergent if we rearrange it in an special way, but he points out that it would be really interesting knowing whether in general this sum is actually absolutely convergent. Indeed, in such a case the sum would be always convergent whatever is the order in which the terms of the summation are, or in other words, we would not have to take care of where we put the brackets. Since only subgroups H with $\mu_G(H) \neq 0$ occur in (1), let us denote by $b_n(G)$ the number of such subgroups of index n. We will say that $b_n(G)$ is polynomially bounded if it is bounded above by n^{α}, for some α independent of n, and we will say that μ_G is polynomially bounded if for every $H \leq G$, the term $|\mu_G(H)|$ is bounded above by $|G : H|^{\beta}$, for some β independent of H. It is shown in [12] that the absolutely convergence of (1) in profinite groups is equivalent to proving that both $b_n(G)$ and μ_G are polynomially bounded.

We will see that if H is a subgroup such that $\mu_G(H) \neq 0$, then it is an intersection of maximal subgroups. Hence, $b_n(G) \leq c_n(G)$, and so, in order to prove that $b_n(G)$ is polynomially bounded, it suffices to prove that actually, $c_n(G)$ is polynomially bounded. This is what motivated Mann to formulate Problem 1, since knowing the answer of it would provide groups in which (1) is absolutely convergent. Nevertheless, the answer of this question is still unknown, and Problem 1 remains being an open problem.

However, when working with finitely generated prosolvable groups (by prosolvable we always mean pro-finite-solvable), the situation is a little better. As said, Mann found a way to rearrange (1) in such a way that it becomes convergent. But it can be said much more. If G is a finitely generated prosolvable group, then, as proved in [10], both μ_G and $b_n(G)$ are polynomially bounded, and so, we can ensure that in this case the series (1) is absolutely convergent. However, even if this solves the principal problem for which Mann posed Problem 1, it does not solve Problem 1 itself. That is, we still do not know if $c_n(G)$ is polynomially bounded in a finitely generated prosolvable group. The aim of this paper will be analysing this case.

Problem 2 (Main Problem)**.** Let G be a finitely generated prosolvable group. Is $c_n(G)$ polynomially bounded?

Even if it will remain being an open problem, we will try to bring us closer to its solution. For that purpose, we will try to follow a similar idea used by Lucchini in [10] to prove that in a finitely generated prosolvable group G, there exists a constant α such that $b_n(G) \leq n^{\alpha}$. In this article, Lucchini proves that if G is a finite solvable group, then, for any subgroup H such that $\mu_G(H) \neq 0$, there exists a family of maximal subgroups $M_1, \ldots, M_t$ of G such that:

i) $H = M_1 \cap \ldots \cap M_t$.

ii) $|G : H| = |G : M_1| \ldots |G : M_t|$.

Using this result and the fact that a finitely generated prosolvable group has polynomial maximal subgroup growth, he concludes saying that for any finitely generated prosolvable group G, the coefficient $b_n(G)$ is polynomially bounded.

With this in mind, we could try to generalise this result for intersections of maximal subgroups instead of for subgroups with non-zero Möbius number, in such a way that we could conclude similarly, saying that in finitely generated prosolvable groups, $c_n(G)$ is polynomially bounded. Thus, we conjecture the following.

Conjecture 1. Does there exist a constant γ with the following property? If G is a finite solvable group, and H a subgroup of G which is an intersection of maximal subgroups of G, then there exists a family of maximal subgroups $M_1, \ldots, M_t$ such that:

i) $H = M_1 \cap \ldots \cap M_t$.

ii) $|G : M_1| \ldots |G : M_t| \leq |G : H|^{\gamma}$.

Proving this conjecture would yield an affirmative answer to Problem 2.

In order to address it, however, we will need some preliminary results. Thus, in Chapter 2, we give a brief introduction to cohomology of finite groups taken mainly from [5], and following principally [2] we will develop the theory of crowns in finite solvable groups. The technical result will be taken from [4], [8] and [16].

Once we have exposed all the theory we need, we will see in Chapter 3 that this conjecture can be solved when assuming some hypothesis. Indeed, we prove that if there exists a constant γ such that for every finite solvable group G, for every irreducible G-module V isomorphic as a G-module to a complemented chief factor of G and for every $W \leq_{\mathrm{End}_G(V)} V$, there exists $W^* \leq_{\mathrm{End}_G(V)} W$ satisfying $C_G(W) = C_G(W^*)$ and $\dim_{\mathrm{End}_G(V)}(W^*) \leq \gamma$, then our conjecture is true. At this point, we could give another conjecture.

Conjecture 2. Does there exist a constant γ with the following property? If G is a finite solvable group, then for every G-module V isomorphic as a G-module to a complemented chief factor of G, and for every $W \leq_{\mathrm{End}_G(V)} V$, there exists $W^* \leq_{\mathrm{End}_G(V)} W$ satisfying:

i) $C_G(W) = C_G(W^*)$.

ii) $\dim_{\mathrm{End}_G(V)}(W^*) \leq \gamma$.

Thus, Conjecture 2 would imply Conjecture 1.

In view of this latter result, in Chapter 4 we will give some examples in which we can ensure that Conjecture 2 holds. Specifically, we will see that it holds in supersolvable groups and also in the more general case of groups with nilpotent derived subgroup. We will also use this section to show a particular example of a prosupersolvable group for which the amount of intersections of maximal subgroups with zero Möbius number is very "big".

Chapter 1

Motivation

In this first chapter we will explain more in detail what we have said in the introduction. Thus, we will follow the same schedule that we have used there, and add also some examples and remarks. In fact, we will start exhibiting some preliminaries, just to fix notation and to know the context we are working on.

The chapter will principally expose the result and discussions of [13] and [10].

1.1 Preliminaries

Let G be a profinite group and consider $P_G(k)$, the probability that k random elements of G generate G.

Definition 1.1. A profinite group G is said to be *positively finitely generated*, or simply PFG, if for some k, the probability $P_G(k)$ that k random elements of G generate G is positive.

Notice that all PFG groups are finitely generated, while the converse is not true. Indeed, the set consisting of k-tuples in G^k that generate G could have measure zero in G^k for every $k \in \mathbb{N}$.

For a finitely generated profinite group G, we will write $a_n(G)$ to express the number of subgroups of index n, and $m_n(G)$ for the number of maximal open subgroups of index n.

Definition 1.2. A profinite group G is said to have *polynomial subgroup growth*, or simply PSG, if there exists $k \geq 0$ such that $a_n(G) \leq n^k$ for every $n \geq 1$. If there exists $k' \geq 0$ such that $m_n(G) \leq n^{k'}$, then we say that G has *polynomial maximal subgroup growth*, or simply PMSG.

Of course, PSG implies PMSG, but the converse is not necessarily true. Nevertheless, we can give a characterization of groups with PMSG as shows the following well-known theorem.

Theorem 1.3. *A profinite group has PMSG if and only if it is PFG.*

Along the dissertation, as seen in the introduction, we will principally work with finitely generated prosolvable and finite solvable groups. Therefore, it is important to know which of the properties defined above are satisfied by them. The following theorem makes it clear. The proof of it can be found in Theorem 10 of [13]. In this proof, Mann uses some results of other papers, such as [15] (that essentially uses a result of Pálfy), which says that the number of conjugacy classes of the maximal solvable subgroups of $\mathrm{GL}(n, p)$ (p prime) is at most $2^{n-1}n^{20\log^3 n+5}$, and [19], which says that if T is a finite solvable group acting irreducibly on a vector space V, then $|T| \leq |V|^{2.25}$.

Theorem 1.4. *Finitely generated prosolvable groups have PMSG, and hence they are PFG.*

It is not true that all prosolvable groups have PSG. For instance, it is proved in [9] (Theorem 3.6) that every non-abelian free pro-p-group has exponential subgroup growth. Nevertheless, by Theorem 12 of [13] we can say that the growth of the subgroups of a finitely generated prosolvable group will not be faster than that, that is, it will be at most exponential.

1.2 The Möbius Function

The so-called Möbius function was firstly defined as a function in number theory by August Ferdinand Möbius in 1832. Nowadays, however, it has been extended to other areas, such as Group Theory, Order theory, Semigroup Theory, etc. In fact, the Möbius function associated to a group G, the one we are working with, is an special case of the Möbius function defined in Order theory, just considering the subgroup lattice of G.

It was firstly introduced by Philip Hall in [7], and he proved that

$$P_G(t) = \sum_{H \leq G} \mu_G(H)/|G : H|^t, \tag{1.1}$$

making clear its importance in Probabilistic Group Theory. As said, Mann tried to generalise this for finitely generated profinite groups. The discussion we present now, which is taken directly from [13], shows what Mann did for this purpose. In addition, if one observes the definition of the Möbius function in the introduction, it is not easy to see at first sight which the real meaning of it could be. This discussion will also explain one of the possible meanings it may have.

Let G be a PFG group. Obviously, a t-tuple generates G if and only if it does not belong to any open maximal subgroup, and the probability for that is

$$1 - \sum \frac{1}{|G : M|^t} + \sum \frac{1}{|G : M \cap L|^t} - \dots \tag{1.2}$$

where M, $L, \dots$ range over all maximal subgroups of G. Observe that this expression makes sense only if each of the infinitely many sums occurring in it converges. Let us rearrange it as follows. First choose a descending open subgroup neighbourhood basis of the identity $\{N_i\}$ (it is easy considering intersections in any open subgroup neighbourhood basis). Let

X_i be the set of maximal open subgroups containing N_i, and note that there are finitely many such maximal for every i. Then, $P_G(t)$ is the limit, as $n \to \infty$, of the probability that a random t-tuple does not lie in a maximal subgroup in the set X_n. This probability is a finite sum, consisting of the terms in (1.2) that involve only maximal subgroups from X_n, and the limit of this sum can be formally rearranged in the form

$$P(G,t) = \sum \mu(H)/|G:H|^t, \tag{1.3}$$

for some coefficients $\mu(H)$, where H ranges over all 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, etc. It is shown in [13] that this series does not depend on the choice of the basis $\{N_i\}$, and that if G is a finitely generated prosolvable group, then it is convergent for t big enough (as we will see later, and as we already have said in the introduction, this series is actually absolutely convergent if G is a finitely generated prosolvable group).

Let us focus on the coefficients $\mu(H)$. Note that a subgroup H can occur in (1.3) with a non-zero coefficient only if H is an intersection of maximal subgroups. In addition, for such a subgroup, $\mu(H)$ is the difference between the number of ways to express H as the intersection of evenly many maximal subgroups and the number of ways to express it as such an intersection of oddly many terms.

By Theorem 1.6 below we know that if H is not an intersection of maximal subgroups then $\mu_G(H) = 0$. With this, and recalling the definition of μ_G, it is easily seen that $\mu(H)$ satisfies the defined equalities of $\mu_G(H)$, and hence, $\mu(H) = \mu_G(H)$.

Example 1.5. If $G = \mathbb{Z}$, one obtains the classical number theoretical Möbius function, setting $\mu_{\mathbb{Z}}(n\mathbb{Z}) = \mu(n)$.

Mann showed in [12] that for profinite groups, proving the absolutely convergence of (1.3) is equivalent to proving that both $b_n(G)$ and μ_G are polynomially bounded. Let us focus on the coefficient $b_n(G)$. The following theorem shows that $b_n(G) \leq c_n(G)$.

Proposition 1.6. *Let G be a group and H a subgroup of G of finite index. If $\mu_G(H) \neq 0$, then H is an intersection of maximal subgroups of G.*

Proof. We proceed by induction on the index of H. The trivial case is obvious, so assume $|G:H| = n > 1$. Since the index is finite, the index of H_G is also finite, and the group G/H_G is a finite group. By the Isomophism Theorems, there is a bijection between all subgroups of G containing H and all subgroups of G/H_G containing H/H_G. So, $\mu_G(H) = \mu_{G/H_G}(H/H_G)$, and we may assume that G is finite. Denote by $M_1, \dots, M_t$ the maximal subgroups of G containing H. Define $U := \cap_{1\leq i \leq t} M_i$. By contradiction, suppose $H < U$. By induction, it follows that all subgroups with non-zero Möbius function in which H is properly contained are intersections of maximal subgroups, and hence, U is contained in all of them. Thus,

$$\begin{aligned}\mu_G(H) &= -\sum_{H<K\leq G} \mu_G(K) = -\sum_{U\leq K\leq G} \mu_G(K) \\ &= -\sum_{U<K\leq G} \mu_G(K) - \mu_G(U) = -\mu_G(U) + \mu_G(U) = 0,\end{aligned}$$

which is a contradiction. Therefore, $H = U$, as we wanted. □

Remark 1.7. It is not difficult to find a counterexample which shows that the converse of this theorem is not true. For instance, consider the group

$$G = \langle a, b \mid a^5 = b^4 = 1, a^b = a^2 \rangle.$$

One can check that the maximal subgroups of this group are $\langle a \rangle \rtimes \langle b^2 \rangle$ and $\langle b \rangle^{a^i}$ for $i = 1, \ldots, 5$. The intersections of the conjugates of $\langle b \rangle$ are pairwise trivial (so $\Phi(G) = 1$), and the intersections of $\langle a \rangle \rtimes \langle b^2 \rangle$ with the conjugates of $\langle b \rangle$ are pairwise distinct of order 2. Note that the Möbius number of a maximal subgroup is always -1, and the Möbius number of the intersection of two maximal subgroups that is not contained in other maximal subgroups is 1. Knowing this, it is easy to check that $\mu_G(1) = 0$, but, as noted before, $1 = \Phi(G)$ is an intersection of maximal subgroups. We also construct in Section 4.1.1 supersolvable groups providing a lot of intersections of maximal subgroups with zero Möbius number.

So, in order to prove that $b_n(G)$ is polynomially bounded, it suffices to prove that so is $c_n(G)$. As said in the introduction, using other methods, Lucchini proves in [10] that for a finitely generated prosolvable group G, both $b_n(G)$ and μ_G are polynomially bounded (and in particular, (1.3) is absolutely convergent in these groups). These "other methods" will be the ones we will try to follow in order to prove that $c_n(G)$ is also polynomially bounded in finitely generated prosolvable groups (or at least in order to get closer to proving it).

1.3 $b_n(G)$ is Polynomially Bounded in Prosolvable Groups

In order to prove that in finitely generated prosolvable groups $b_n(G)$ is polynomially bounded, we will expose the results in [10]. As we will see, the key to prove that $b_n(G)$ is polynomially bounded will be Theorem 1.12.

Let G be a finite group. To any subgroup of H of G, there corresponds a Dirichlet polynomial $P_G(H, t)$ defined as follows:

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

The term $P_G(H, t)$ represents the probability that t random elements, together with H, generate G. The following remark is clear.

Remark 1.8. If $a_n(G, H) \neq 0$, then $n \leq |G : H|$. Moreover, $\mu_G(H) = a_{|G:H|}(G, H)$.

Let N be a normal subgroup of G. Then, we may consider the Dirichlet polynomial $P_{G/N}(HN/N, t)$. The following proposition, which is proved in [11] (Proposition 16), shows that $P_{G/N}(HN/N, t)$ divides $P_G(H, t)$ and says which is the divisor.

Proposition 1.9. *If N is a normal subgroup of a finite group G, then*

$$P_G(H, t) = P_{G/N}(HN/N, t) P_{G,N}(H, t),$$

where

$$P_{G,N}(H,t) := \sum_{n\in\mathbb{N}} \frac{b_n(G,H,N)}{n^t} \quad \textit{with} \quad b_n(G,H,N) := \sum_{\substack{|G:K|=n \\ H\leq K\leq G, KN=G}} \mu_G(K).$$

Remark 1.10. If $b_n(G,H,N) \neq 0$, then there exists K such that

$$n = |G : K| = |N : K \cap N| \leq |N : H \cap N|.$$

Lemma 1.11. *Let G be a finite group, H a subgroup of G and N a normal subgroup of G. If $\mu_G(H) \neq 0$, then the following holds:*

i) $\mu_G(HN) \neq 0$

ii) There exists $K \leq G$ such that $H \leq K$, $KN = G$ and $H \cap N = K \cap N$.

Proof. Assume $\mu_G(H) = a_{|G:H|}(G,H) \neq 0$. By Proposition 1.9, there exist positive integers u and v such that $a_u(G/N, HN/N) \neq 0$, $b_v(G,H,N) \neq 0$ and $uv = |G : H|$. By Remark 1.8 we have $u \leq |G : HN|$, and by Remark 1.10 we have $v \leq |N : H \cap N|$. In addition,

$$|G : H| = |G : HN||HN : H| = |G : HN||N : H \cap N|,$$

and since $|G : H| = uv$, it follows that $u = |G : HN|$ and $v = |N : H \cap N|$. Observe that $\mu_{G/N}(HN/N) = \mu_G(HN)$, so we have

$$0 \neq a_{|G:HN|}(G/N, HN/N) = \mu_{G/N}(HN/N) = \mu_G(HN),$$

as we wanted.

For part *ii*), note that since $b_v(G,H,N) = b_{|N:H\cap N|}(G,H,N) \neq 0$, then there exists K with $H \leq K$, $KN = G$ and

$$|G : K| = |N : K \cap N| = |N : H \cap N|.$$

Clearly, we must have $K \cap N = H \cap N$. □

Even if the part *i*) of the following theorem is proved in Proposition 1.6, we will use different arguments to prove it for solvable groups. In fact, this different way of proving it will provide a particular family of maximal subgroups for which the assertion of part *ii*) of the theorem will be satisfied.

Theorem 1.12. *Let G be a finite solvable group and let H be a subgroup of G with $\mu_G(H) \neq 0$. Then, there exists a family $M_1, \ldots, M_t$ of maximal subgroups of G such that:*

i) $H = M_1 \cap \ldots \cap M_t$.

ii) $|G : H| = |G : M_1| \ldots |G : M_t|$.

Proof. The theorem will be proved by induction on $|G : H|$. For $H = G$ the result is clear, so let us proceed with the general case. The definition of $\mu_G(H)$ only takes into account the subgroups over H, which means that

$$\mu_G(H) = \mu_{G/H_G}(H/H_G),$$

so that we may assume $H_G = 1$. Let N be a minimal normal subgroup of G, which of course is not contained in H. Recall that N is abelian since G is solvable. By the previous lemma, $\mu_G(HN) \neq 0$, and there exists K such that $H \leq K$, $G = KN$ and $K \cap N = H \cap N$. Note that since N is normal in G, then $K \cap N = H \cap N$ is normal in K and since N is abelian, $K \cap N = H \cap N$ is also normal in N. As said, $G = KN$, so that $K \cap N = H \cap N$ is normal in G. As $H_G = 1$, we conclude that $K \cap N = H \cap N = 1$. In particular, K is a maximal subgroup of G and

$$|G : K| = |N| = |N : H \cap N| = |HN : H|.$$

If $G = HN$, then $H = K$ would be a maximal subgroup of G and we would be done, so assume $HN < G$. Thus, by induction, there exists a family $M_1, \ldots, M_u$ of maximal subgroups of G such that

$$HN = \bigcap_{1 \leq i \leq u} M_i \qquad \text{and} \qquad |G : HN| = \prod_{1 \leq i \leq u} |G : M_i|.$$

By the Dedekind Law, we have $HN \cap K = H(N \cap K) = H$, and so,

$$H = M_1 \cap \ldots \cap M_u \cap K.$$

Moreover,

$$|G : H| = |G : HN||HN : H| = |G : HN||G : K| = |G : M_1| \ldots |G : M_u||G : K|.$$

Thus, $M_1, \ldots, M_u, K$ is the required family of maximal subgroups of G, and we are done. □

We can finally prove the following theorem.

Theorem 1.13. *Let G be a finitely generated prosolvable group. Then, there exists a constant β such that $b_n(G) \leq n^\beta$.*

Proof. By Theorem 1.4 we know that G has PMSG, which means that there exists α such that for each $n \in \mathbb{N}$, we have $m_n(G) \leq n^\alpha$. Now, for $n \neq 1$, we want to count the number of subgroups H with $|G : H| = n$ and $\mu_G(H) \neq 0$. By Theorem 1.12, for each H of this type, there exists a family of maximal subgroups $M_1, \ldots, M_t$ such that $H = \cap_{1 \leq i \leq t} M_i$ and $n = n_1 \ldots n_t$, where $n_i = |G : M_i|$. There are at most n possible factorizations of n (see [14]), and for each fixed factorization $n = n_1 \ldots n_t$, there are at most n_i^α choices for the maximal subgroup M_i corresponding to n_i. Therefore, there are at most $n_1^\alpha \ldots n_t^\alpha = n^\alpha$ choices for the family $M_1, \ldots, M_t$, and we conclude that $b_n(G) \leq n^{\alpha+1}$. □

This procedure will be the one we will try to follow when working with $c_n(G)$ instead of $b_n(G)$. Nevertheless, the results we will expose will require some preliminaries, such as some basic result on cohomology and, specially, the important notion of the crown in finite solvable groups. The following chapter is dedicated to develop all these requirements before addressing the issue.

Chapter 2

Cohomology of Finite Groups and Crowns in Finite Solvable Groups

Along this dissertation, as said, the notion of crown in finite solvable groups will be of great importance. However, before defining it, some basic results on cohomology of finite groups are needed for the purpose of obtaining interesting results about such crowns in finite solvable groups. This chapter is dedicated to, firstly, develop such a theory, and then to define the crowns and prove some properties of them.

2.1 G-modules

We rapidly give some straightforward definitions about G-modules, which are very similar to other algebraic structures. These notions will be necessary to define the concept of cohomology.

Definition 2.1. Let G be a finite group. We say that an abelian finite group V is a *G-module* if there exists a map $(v, g) \to v^g$ of $V \times G$ in V such that for every $v, v_1, v_2 \in V$ and $g, g_1, g_2 \in G$ we have:

i) $(v_1 + v_2)^g = v_1^g + v_2^g$.

ii) $v^1 = v$.

iii) $v^{(g_1 g_2)} = (v^{g_1})^{g_2}$.

Notation 2.2. If U is a subgroup of V and H is a subgroup of G, we will write

$$U^H = \{u^h \mid u \in U, h \in H\}.$$

Definition 2.3. Let G be a finite group. A subgroup W of a G-module V is said to be a *G-submodule* of V, and we write $W \leq_G V$, if for every $w \in W$ and $g \in G$ we have $w^g \in W$, or equivalently, if $W^G = W$. If $W \leq_G V$, then V/W can be seen as a G-module by setting

$$(v + W)^g = v^g + W,$$

where $v \in V$ and $g \in G$.

Definition 2.4. Let G be a finite group. A G-module V is *irreducible* or *simple* if the only proper G-submodule of V is 0. A G-module is said to be *completely reducible* or *semisimple* if for every G-submodule W of V there exists a G-submodule U of V such that $V = W \oplus U$.

If V is a finite G-module, one can easily check that it is completely reducible if and only if it is a direct sum of finitely many finite irreducible G-modules.

Definition 2.5. Let G be a finite group and let V and W be G-modules. A *homomorphism of G-modules* between V and W is a group homomorphism ϕ such that $\phi(v^g) = \phi(v)^g$ for every $v \in V$ and $g \in G$. We say that ϕ is an *isomorphism of G-modules* between V and W if it is a G-homomorphism and an isomorphism of groups. In this case, V and W are said to be *isomorphic as G-modules*, or *G-isomorphic.*

By repeating the same proofs for G-modules instead of for groups, one can easily verify that the three isomorphism theorems of groups are also satisfied when working with G-modules.

We can define a group to be a *G-group* in the same way as we have defined the G-modules but without asking them to be abelian. That is, G-groups are a generalization of G-modules. We can also define G-homomorphisms and G-isomorphisms in the same way. For example, a non-abelian normal subgroup of G is a G-group, but it is not a G-module. In this case, the three isomorphism theorems are also satisfied, and furthermore, if one of these ways of constructing new G-isomorphic groups creates an abelian group, then the resulting G-isomorphism will be also an isomorphism between G-modules. These two terms will arise naturally again and again, and we will use them without mention of any specific detail. Indeed, we will often use the term G-homomorphism (G-isomorphism) when talking about homomorphisms (isomorphisms) of G-modules.

Notation 2.6. The set of all G-homomorphisms from a G-module V to another G-module W is denoted by $\mathrm{Hom}_G(V, W)$. If $V = W$, it is denoted simply by $\mathrm{End}_G(V)$.

Remark 2.7. One can give abelian group structure to the set $\mathrm{Hom}_G(V, W)$, and in particular to $\mathrm{End}_G(V)$, by setting

$$(\phi_1 + \phi_2)(v) = \phi_1(v) + \phi_2(v) \quad \text{and} \quad (-\phi)(v) = -\phi(v),$$

for every $\phi_1, \phi_2, \phi \in \mathrm{Hom}_G(V, W)$ and $v \in V$. Indeed, it is routine checking that $\phi_1 + \phi_2$ and $-\phi$ are contained in $\mathrm{Hom}_G(V, W)$.

Furthermore, by Schur's lemma, we can ensure that if V and W are two irreducible G-modules, then a G-homomorphism $\phi : V \longrightarrow W$ is either 0 or a G-isomorphism. In particular, if V and W are not G-isomorphic, then $\mathrm{Hom}_G(V, W) = 0$, but on the contrary, $\mathrm{End}_G(V)$ can be seen as a division ring with the addition and the composition. Moreover, since V is finite, so is $\mathrm{End}_G(V)$, so from Weddeburn's theorem follows that it is a field.

Definition 2.8. Let G be a finite group and V a G-module. The *submodule of G-invariant elements* is the subset

$$V_G = \{v \in V \mid v^g = v \text{ for every } g \in G\}.$$

It is straightforward checking that V_G is a G-submodule of V.

It is well known that in p-groups there is no normal subgroup intersecting trivially with the center. The following theorem generalises this result. The proof is omitted since it is very similar to that of p-groups.

Theorem 2.9. *Let G be a finite p-group and let V be a G-module such that $|V| = p^r$ for some integer r. If $0 \neq W \leq_G V$, then $V_G \cap W \neq 0$.*

Definition 2.10. Let G be a finite group and V a G-module. The *centralizer* of $W \subseteq V$ in G, denoted $C_G(W)$, is the subset

$$C_G(W) = \{g \in G \mid w^g = w \text{ for every } w \in W\}.$$

If $C_G(V) = 1$, then we say that V is a *faithful* G-module.

The centralizer $C_G(V)$ of a G-module V is obviously a normal subgroup of G since it can be seen as the kernel of the homomorphism

$$\begin{aligned} \phi : G &\longrightarrow \mathrm{Aut}(V) \\ g &\longrightarrow (v \rightarrow v^g). \end{aligned}$$

Moreover, if N is a normal subgroup of G lying in $C_G(V)$, then V can be seen, in a natural way, as a G/N-module. Furthermore, an isomorphism of V into another G-module W is a G-isomorphism if and only if it is a G/N-isomorphism.

To end this section, we introduce a G-module that will be constantly used along this work. Let K and H be two normal subgroups of G such that $K \leq H$ with H/K abelian. Then H/K can be seen as a G-module setting

$$(hK)^g = h^g K,$$

for $g \in G$. In this case, $C_G(H/K) \geq H$. In addition, H/K is a chief factor of G if and only if it is an irreducible G-module. In the case in which G is solvable, since a chief factor H/K is a minimal normal subgroup of the solvable group G/K, it follows that H/K is abelian. We will say that a chief factor H/K is *Frattini* if it is contained in the Frattini subgroup of G/K. On the contrary, we will say that a chief factor H/K is *complemented* if it is complemented in G/K.

2.2 Cohomology of Finite Groups

Knowing all this, we are now ready to start defining the cohomology groups of a finite group G with coefficients in a G-module V.

It is not easy to say who defined first the cohomology groups, since it has been introduced in different areas for different reasons. The first theorem of the subject could be identified as Hilbert's Theorem 90 in 1897, even if the notion of group cohomology was not formulated until 1943-45. Nowadays it is as an area of active research.

We will first give a brief theoretical definition in order to have a better understanding of the concept. However, since the aim of this dissertation does not need deep results in cohomology, we immediately will show explicitly how these cohomology groups look like, and we will always work with this definition.

In the theoretical definition we use some concepts of category theory. If the reader is not familiar with these notions, he or she can directly read the explicit definition.

Let G be a finite group, and let V be a G-module. Sending V to its G-submodule V_G of G-invariant elements yields a functor F from the category of G-modules to the category of abelian groups. One can check that this functor is left exact, so we could consider its right derived functors R^iF.

Definition 2.11. In the notation above, we define $H^i(G,V) = R^iF(V)$. It is obviously an abelian group, and it is called the ith cohomology group of G with coefficients in V.

Clearly, $H^0(G,V) = V_G$. Notice that if we see $\mathbb{Z}$ as a trivial G-module (every $g \in G$ acts trivially on every $z \in \mathbb{Z}$), then $V_G \cong \mathrm{Hom}_G(\mathbb{Z}, V)$ via the homomorphism

$$\begin{aligned} \mathrm{Hom}_G(\mathbb{Z}, V) &\longrightarrow V_G \\ \varphi \quad &\longrightarrow \varphi(1). \end{aligned}$$

Therefore, recalling that the derived functors of Hom are the so called Ext-functors, we have $H^i(G,V) \cong \mathrm{Ext}^i_G(\mathbb{Z}, V)$.

This, as said, is a very conceptual definition, which allows us to understand what the cohomology is, but does not help too much in concrete applications. As promised before, we show now explicitly which form have the cohomology groups, although we will not prove the equivalence between both definitions.

For every $i \geq 0$, let $C^i(G,V)$ be the set of all functions from G^i to V (here, G^0 means a singleton, so that $C^0(G,V) \cong V$). We can give abelian group structure to this set by setting

$$(\phi_1 + \phi_2)(g) = \phi_1(g) + \phi_2(g) \qquad \text{and} \qquad (-\phi)(g) = -\phi(g)$$

for every $\phi_1, \phi_2, \phi \in C^i(G,V)$ and $g \in G^i$. We define the homomorphisms

$$d^i : C^i(G,V) \longrightarrow C^{i+1}(G,V)$$

by

$$\begin{aligned} (d^i\phi)(g_0, g_1, \dots, g_i) = {} & \phi(g_0, \dots, g_{i-1})^{g_i} \\ & + \sum_{j=0}^{i-1} (-1)^{j+1} \phi(g_0, \dots, g_{i-j-2}, g_{i-j-1}g_{i-j}, \dots, g_i) \\ & + (-1)^{i+1} \phi(g_1, \dots, g_i). \end{aligned}$$

It is easy to check by routine computations that $d^{i+1} \circ d^i = 0$, so this means we actually have a chain complex of abelian groups

$$V \xrightarrow{d^0} C^1(G,V) \xrightarrow{d^1} C^2(G,V) \xrightarrow{d^2} \cdots \xrightarrow{d^{i-1}} C^i(G,V) \xrightarrow{d^i} C^{i+1}(G,V) \xrightarrow{d^{i+1}} \cdots .$$

Definition 2.12. The cohomology groups of the chain complex constructed above are called the cohomology groups of G with coefficients in V, and denoted by $H^i(G, V)$.

Therefore, as this definition says,

$$H^i(G, V) = \frac{Z^i(G, V)}{B^i(G, V)},$$

where $Z^i(G, V) = \ker d^i$ and $B^i(G, V) = \text{Im } d^{i-1}$.

The following proposition can be proved easily.

Proposition 2.13. *Let G be a finite group and let V and W be two G-modules. Then,*

$$H^i(G, V \oplus W) = H^i(G, V) \oplus H^i(G, W).$$

By knowing some results concerning the first cohomology group of a finite group G, we will be able to deduce interesting properties of it. In order to do this, we must know how this cohomology group is. So, let us compute it explicitly.

As said, we have to compute $Z^1(G, V)$ and $B^1(G, V)$. By definition, for $\phi \in C^1(G, V)$, we have $(d^1\phi)(g_0, g_1) = \phi(g_0)^{g_1} - \phi(g_0g_1) + \phi(g_1)$, so

$$Z^1(G, V) = \ker d^1 = \{\phi \in C^1(G, V) \mid \phi(gh) = \phi(g)^h + \phi(h) \text{ for every } g, h \in G\}.$$

On the other hand, for $v \in V$ we have $(d^0g)(g_0) = vg_0 - v$, so

$$B^1(G, V) = \text{Im } d^0 = \{\phi \in C^1(G, V) \mid \text{there exists } v \in V \text{ such that } \phi(g) = v^g - v\}.$$

Proposition 2.14. *Let G be a finite group and let V be a G-module. Then, for every $n \in \mathbb{N}$ we have:*

i) $\exp(H^n(G, V)) \mid |G|$

ii) $\exp(H^n(G, V)) \mid \exp(V)$

Proof. For simplicity, we will prove part i) only for $H^1(G, V)$. In fact, along the paper we will only use this proposition in such a case. Using the construction above, let $\phi \in Z^1(G, V)$. Then, for every $h \in G$, we have $\phi(h) = \phi(gh) - \phi(g)^h$ for every $g \in G$. Thus,

$$|G|\phi(h) = \sum_{g\in G} \phi(gh) - \sum_{g\in G} \phi(g)^h = \sum_{g\in G} \phi(g) - (\sum_{g\in G} \phi(g))^h.$$

Taking $v = -\sum_{g\in G} \phi(g)$ we deduce $|G|\phi \in B^1(G, V)$. Therefore, $\exp(H^1(G, V)) \mid |G|$.

For the second part, just observe that for every $\phi \in C^n(G, V)$ and for every $g \in G^n$, we have $\phi(g) \in V$. So, $\exp(V)\phi(g) = 0$ for every $\phi \in C^n(G, V)$ and for every $g \in G^n$. □

Let G be a group written multiplicatively. Let V a normal abelian subgroup of G and H a finite subgroup of G complementing V. Then, H can act on V via conjugation in such a way that V becomes an H-module.

Theorem 2.15. *In the situation above, $|H^1(H,V)|$ is equal to the number of conjugacy classes of the complements of V in G. In particular, if $H^1(H,V)$ is trivial, then all the complements of V in G are conjugate.*

Proof. Let H' be a complement of V in G. Then, since H also complements V, for every $h' \in H'$ we can find two unique elements $x \in H$ and $v_x \in V$ such that $h' = xv_x$. We define the function $\phi : H \to V$ by $\phi(x) = v_x$, so that

$$H' = \{x\phi(x) \mid x \in H\}.$$

For every $x, y \in H$ we have $x\phi(x)y\phi(y) = xy\phi(x)^y\phi(y)$, and since V is normal in G, then $\phi(x)^y\phi(y) \in V$. So, $\phi(xy) = \phi(x)^y\phi(y)$. This means that the functions ϕ that can arise for different conjugates are exactly those of $Z^1(H,V)$ (note that in this case we are writing the operation multiplicatively).

Now, H' is a conjugate of H if and only if $x\phi(x) = x^v = x(v^{-1})^x v$ for every $x \in H$ and a suitable $v \in V$. So, $\phi(x) = (v^{-1})^x v$ and actually $\phi \in B^1(H,V)$. The result follows now easily. □

Before ending this section we will give a result concerning exact sequences of G-modules. However, its proof requires some preliminaries, so it will be omitted. One could find the proof in [5].

Lemma 2.16. *Let G be a finite group and let V be a G-module. Then, for every $N \trianglelefteq G$, the sequence*

$$0 \longrightarrow H^1(G/N, V_N) \longrightarrow H^1(G,V) \longrightarrow H^1(N,V)$$

is exact.

2.3 Crowns in Finite Solvable Groups

Since we are interested in solvable groups, we dedicate this section to exposing some important properties of them. In particular, we will show what the crowns are, and we will give some very useful results related with them. In order to prove them, the already proved theorems of the previous chapter concerning cohomology will be really helpful.

We start with a proposition which generalises the well known property of having prime power order of the minimal normal subgroups of a solvable group. The proof is omitted since it is very similar to that of minimal normal subgroups.

Proposition 2.17. *Let G be a finite solvable group and let V be an irreducible G-module. Then $|V| = p^r$ for some prime p and some integer r.*

Theorem 2.19 below will allow us to use Theorem 2.15 when working with some kind of chief factors of finite solvable groups. Before proving it, however, we need a lemma.

Lemma 2.18. *Let G be a solvable group and let V be an irreducible G-module of order p^r. Then, $G/C_G(V)$ has not any normal proper p-subgroup.*

Proof. By contradiction, assume there exists a subgroup N such that $C_G(V) < N \trianglelefteq G$ and $N/C_G(V)$ is a p-group. Since V is irreducible, it follows that $V_N = V$ or $V_N = 0$. However, by Theorem 2.9, considering V as a $N/C_G(V)$-module, we have $V_N \neq 0$. So $V_N = V$, and hence $N \leq C_G(V)$, which is a contradiction. □

Theorem 2.19. *Let G be a finite solvable group and V an irreducible G-module. If $C_G(V) = 1$, then $|H^1(G, V)| = 1$.*

Proof. If $G = 1$ it is obvious, so assume $G \neq 1$. Assume also $|V| = p^r$ for some prime p and some integer r, and let N be a minimal normal subgroup of G. By Lemma 2.18, we have $(|N|, p) = 1$. Therefore, by Theorem 2.14, we have $H^1(N, V) = 0$. In addition, since V is irreducible, $V_N = V$ or $V_N = 0$. If $V_N = V$, then $N \leq C_G(V) = 1$, which is a contradiction, so we have $V_N = 0$. By Lemma 2.16 we deduce that the sequence

$$0 \longrightarrow H^1(G/N, V_N) \longrightarrow H^1(G, V) \longrightarrow H^1(N, V)$$

is exact. In our case $0 \to 0 \to H^1(G, V) \to 0$ is exact. Therefore, $H^1(G, V) = 0$ and we are done. □

Corollary 2.20. *Let G be a solvable group and let M/N be a chief factor of G. If $C_G(M/N) = M$, then M/N is complemented in G/N and all its complements are conjugate.*

Proof. We can always work modulo N, so we will assume $N = 1$, that is, $M/N = M$ and $G/N = G$. Of course, M is a minimal normal subgroup of G, and since G is solvable, $|M| = p^r$ for some prime p and some $r \in \mathbb{N}$. Consider the factor group G/M, and take a minimal normal subgroup L/M of G/M. Again, $|L/M| = q^s$ for some prime q and some $s \in \mathbb{N}$.

If $p = q$, then L is a p-group, and since $Z(L)$ is normal in G, we have $M \cap Z(L) = M$. Then, $L \leq C_G(M) = M$ which is a contradiction.

So, assume $p \neq q$. Let Q be the Sylow q-subgroup of L. Clearly $L = QM$. By the Frattini Argument we have

$$G = LN_G(Q) = QMN_G(Q) = MN_G(Q).$$

Since M is abelian, $M \cap N_G(Q)$ is normal in both M and $N_G(Q)$, so it is normal in G. By minimality of M we have either $M \cap N_G(Q) = 1$ or $M \leq N_G(Q)$. In the first case $N_G(Q)$ would be the desired complement of M, so we would be done. So, assume $M \leq N_G(Q)$. Observe that $M \cap Q = 1$, and since $M \leq N_G(Q)$, then Q is normal in $MQ = L$. Thus, $L = MQ = M \times Q$, and in particular, $Q \leq C_G(M) = M$, which is a contradiction. Thus, we have proved that M/N is complemented in G/N.

Now, recall that M/N is irreducible as a G/M-module, and by Theorem 2.19 we have

$$|H^1(G/M, M/N)| = 1.$$

So, by Theorem 2.15 we get the result. □

The following lemma will be helpful when proving some results.

Lemma 2.21. *Let G be a solvable group and M a maximal subgroup of G. Then, the group G/M_G has a unique minimal normal subgroup N/M_G, and in addition, $C_G(N/M_G) = N$. Moreover, if H/K is a chief factor complemented by the maximal subgroup M/K of G/K, then*

$$H/K \cong_G N/M_G = C_G(N/M_G)/M_G = C_G(H/K)/M_G,$$

where N/M_G is the unique minimal normal subgroup of G/M_G.

Proof. Consider the subgroup HM_G/M_G of G/M_G. Since $H \cap M_G$ is normal in G and K is contained in both H and M_G, we have

$$H \cap M_G = K,$$

and then,

$$HM_G/M_G \cong H/K.$$

Notice that they are also isomorphic as G-modules, so HM_G/M_G is an abelian minimal normal subgroup of G/M_G complemented by M, and $HM_G \leq C_G(HM_G/M_G)$. Note that $C_G(HM_G/M_G) \cap M$ is normal in G since it is normalized by both M and HM_G. Therefore, since M/M_G is core-free in G/M_G, we have $C_G(HM_G/M_G) \cap M = M_G$. Now,

$$C_G(HM_G/M_G) = C_G(HM_G/M_G) \cap HM_GM = HM_G(C_G(HM_G/M_G) \cap M) = HM_G.$$

Thus,

$$C_G(H/K)/M_G = C_G(HM_G/M_G)/M_G \cong_G H/K,$$

as asserted. □

From now on we will be constantly working with chief factors. Thus, it would be interesting knowing some useful properties of them. In fact, our next goal will be proving a form of the Jordan-Hölder Theorem, which says that in any two chief series of a finite group G, there exists a bijection between the chief factors of them, such that two correspondent chief factors are G-isomorphic. In this case, we will prove even more. We will show that a chief factor of one of our chief series is a Frattini chief factor if and only if so it is the corresponding chief factor of the other chief series. The proof, however, will require three technical lemmas, which we expose now.

Lemma 2.22. *Let G be a finite group. If $N \trianglelefteq G$, $H \leq G$ and $N \leq \Phi(H)$, then $N \leq \Phi(G)$.*

Proof. By contradiction, assume $N \nleq \Phi(G)$. Then, there exists a maximal subgroup M of G not containing N, and $G = NM$. By the Dedekind Law we have

$$H = H \cap NM = N(H \cap M),$$

and since $N \leq \Phi(H)$, it follows that $H = H \cap M$. Thus, $N \leq H \leq M$, which is a contradiction. □

Lemma 2.23. *Let K and N be abelian normal subgroups of a finite group G such that K/N is a chief factor of G and N is a minimal normal subgroup of G. If $K/N \leq \Phi(G/N)$, then $K \leq \Phi(G)N$.*

Proof. If $N \leq \Phi(G)$, then $\Phi(G/N) = \Phi(G)/N$, so the lemma follows trivially. So, suppose that $N \not\leq \Phi(G)$. Since N is not Frattini, there exists a maximal subgroup M not containing it, and since $N \cap M$ is normal in both M and N (recall that N is abelian), then it is normal in $G = NM$. Note that $M \cong G/N$, and this isomorphism yields $\Phi(M)N/N = \Phi(G/N)$. Therefore, $K \leq \Phi(M)N$.

Note now that $\Phi(M) \cap K$ is normalized by M and is also centralized by N, so it is normal in G. Therefore, from Lemma 2.22 we can conclude that $\Phi(M) \cap K \leq \Phi(G)$. Consequently, we obtain

$$K = \Phi(M)N \cap K = (\Phi(M) \cap K)N \leq \Phi(G)N.$$

□

Lemma 2.24. *Let N_1 and N_2 be two distinct minimal normal subgroups of a finite group G. Then there exists a bijection*

$$\sigma : \{N_1, N_1N_2/N_1\} \longrightarrow \{N_2, N_1N_2/N_2\}$$

such that corresponding chief factors are G-isomophic and Frattini chief factors correspond to one another.

Proof. Write $N := N_1N_2$. Let us assume first $N_1 \leq \Phi(G)$. Then, it is known that since N_2 is normal, $N_1N_2/N_2 \leq \Phi(G)N_2/N_2 \leq \Phi(G/N_2)$. If N/N_1 is also Frattini, since $N_1 \leq \Phi(G)$, we have $N \leq \Phi(G)$, and so all four factors in the statement are Frattini. In this case, the map σ with $\sigma(N_1) = N/N_2$ and $\sigma(N/N_1) = N_2$ satisfies the stated requirements. If, on the other hand, N/N_1 is not Frattini, then N_2 is not Frattini (just repeating the arguments used before), and the same choice of σ will suffice. Likewise if all chief factors are not Frattini.

It remains to consider the case in which N_1 and N_2 are non-Frattini and (say) N/N_2 is Frattini. The Frattini subgroup of a finite group is always nilpotent, so in particular, so is $\Phi(G/N_2)$. Therefore, the minimal normal subgroup N/N_2 is abelian and hence so is N_1. Since it is not Frattini, there exists a maximal subgroup M not containing N_1, and since $M \cap N_1$ is normal in both M and N_1 (recall that N_1 is abelian), then so it is in G. This means that $M \cap N_1 = 1$, so actually M is a complement of N_1. Let $N_3 := M \cap N$. Then, by the Dedekind Law,

$$N_3N_1 = (M \cap N)N_1 = MN_1 \cap N = N,$$

and so, $N/N_1 \cong N_3$. If $N_3 = N_2$, then M/N_2 is a complement in G/N_2 to N/N_2, which is a contradiction to the fact that N/N_2 is Frattini. Hence, $N_3 \neq N_2$, and we have $N = N_3N_2$ and $N_3 \cong N/N_2 \cong N_1$. Consequently, N_3 is abelian, and since $N = N_1N_3 \cong N_1 \times N_3$, then N is also abelian. By Lemma 2.23 we have $N_2(N \cap \Phi(G)) = N \cap N_2\Phi(G) = N$, so it follows that $N \cap \Phi(G) = N_3$. Therefore, $N/N_1 = N_3N_1/N_1$ is Frattini, and all four chief factors in question are G-isomorphic. If we then take $\sigma(N_1) = N_2$ and $\sigma(N/N_1) = N/N_2$, we are done. □

Theorem 2.25. *Let G be a finite group. Then, for any two chief series of G*

$$G = X_0 > X_1 > \ldots > X_n = 1 \qquad \textit{and} \qquad G = Y_0 > Y_1 > \ldots > Y_m = 1$$

we have:

i) $n = m$, and there exists $\sigma \in Sym(n)$ such that

$$X_i/X_{i-1} \cong_G Y_{\sigma(i)}/Y_{\sigma(i)-1}.$$

ii) X_i/X_{i+1} is a Frattini chief factor of G if and only if so is $Y_{\sigma(i)}/Y_{\sigma(i)+1}$.

Proof. We will prove both assertions together. Let us call $\mathcal{L}_1$ and $\mathcal{L}_2$, respectively, to our chief series. We will prove it by induction on the sum of the lengths of the composition series. If $n + m = 0$ it is trivial, so let $n + m \geq 1$. If $X_{n-1} = Y_{m-1}$, then we can apply inductive hypothesis to G/X_{n-1}. Thus, we have a suitable correspondence between the chief factors lying above X_{n-1}, and making X_{n-1} correspond to Y_{m-1} we have the result.

Therefore, assume that the minimal normal subgroups X_{n-1} and Y_{m-1} are distinct, and define $N := X_{n-1}Y_{m-1}$. Since $X_{n-1} \cap Y_{m-1} = 1$, it follows that N/X_{n-1} and N/Y_{m-1} are chief factors of G, and there exist two chief series of the form

$$G = Z_0 > Z_1 > \ldots Z_k > N > X_{n-1} > X_n = 1$$

and

$$G = Z_0 > Z_1 > \ldots Z_k > N > Y_{m-1} > Y_m = 1.$$

Let us call them $\mathcal{L}_3$ and $\mathcal{L}_4$ respectively. We will say that two chief series are "equivalent" if they satisfy the requirements of this theorem. Observe that being equivalent is a transitive property. Since the series $\mathcal{L}_1$ and $\mathcal{L}_3$ have the minimal normal subgroup X_{n-1} in common, as proved before, they are equivalent. Similarly, $\mathcal{L}_2$ and $\mathcal{L}_4$ are equivalent. Finally, as the series $\mathcal{L}_3$ and $\mathcal{L}_4$ coincide above N, it clearly follows from Lemma 2.24 that they are also equivalent. Therefore, $\mathcal{L}_1$ and $\mathcal{L}_2$ are equivalent, as desired. □

Remark 2.26. Note that if G is solvable, then a chief factor is Frattini if and only if it is complemented. So, in that case, we can replace "Frattini" by "complemented" in part *ii)* of the previous theorem.

Now we are ready to define the crowns. The concept of crown of a solvable group was firstly introduced by Gaschütz in [6] when he was analysing the structure of the chief factors of a solvable group G as G-modules. However, the notion of crown had been used implicitly on previous papers of Gaschütz himself.

Definition 2.27. Let G be a finite solvable group and V an irreducible G-module. Let

$$\Delta(G,V) := \{N \trianglelefteq G \mid N \leq C_G(V), C_G(V)/N \cong_G V\}$$

and write $R_G(V) := \bigcap_{N \in \Delta(G,V)} N$ or $R_G(V) := C_G(V)$ if $\Delta(G,V) = \emptyset$. The factor group $C_G(V)/R_G(V)$ is called the *crown* of V.

Remark 2.28. If $R_G(V) \neq C_G(V)$, then there exists a chief factor $C_G(V)/N$ isomorphic to V as a G-module, so if $R_G(V) \neq C_G(V)$, we can restrict our choice of an irreducible G-module to a chief factor of G. Recall that these chief factors are abelian since G is solvable.

The definition of crown can be extended to the non-abelian case (see [2]), that is, to the case in which we choose a non abelian chief factor of G instead of a G-module (and of course, G is not solvable). However, since this dissertation is focused on solvable groups, we will restrict ourselves to the abelian case.

Until the end of this chapter we will use the notation introduced in Definition 2.27. In other words, G will be a finite solvable group, V an irreducible G-module and $C_G(V)/R_G(V)$ the crown associated to V.

Next theorem shows how these crowns look like.

Theorem 2.29. *The crown $C_G(V)/R_G(V)$ is isomorphic as a G-module to the direct product of some copies of V, i.e.,*

$$C_G(V)/R_G(V) \cong_G V^{\delta_G(V)},$$

for some $\delta_G(V) \geq 0$.

Proof. If $\Delta(G,V) = \emptyset$ it is obvious, so assume $\Delta(G,V) \neq \emptyset$. Let $N_1, \ldots, N_s$ be the normal subgroups contained in $\Delta(G,V)$, and write $U_j = \cap_{1 \leq i \leq j} N_i$ for $1 \leq j \leq s$ and $U_0 = C_G(V)$. Reordering the N_i subgroups, we may assume

$$N_1 = U_1 > U_2 > \ldots > U_{\delta_G(V)} = U_{\delta_G(V)+1} = \ldots = U_s = R_G(V)$$

for some $1 \leq \delta_G(V) \leq s$. Thus, if we define a G-homomorphism

$$\phi : C_G(V) \longrightarrow \prod_{i=1}^{\delta_G(V)} C_G(V)/N_i \cong_G V \times \overset{\delta_G(V)}{\cdots} \times V = V^{\delta_G(V)}$$

by $\phi(g) = (gN_i)_{1 \leq i \leq \delta_G(V)}$, the kernel of ϕ is then $U_{\delta_G(V)} = R_G(V)$. This means that the crown $C_G(V)/R_G(V)$ is G-isomorphic to a G-submodule of $V^{\delta_G(V)}$.

Let us prove that $|C_G(V)/R_G(V)| = |V|^{\delta_G(V)}$. For every $1 \leq i \leq \delta_G(V)$, note that $U_{i-1}N_i = C_G(V)$, so we have

$$\frac{U_{i-1}}{U_i} = \frac{U_{i-1}}{U_{i-1} \cap N_i} \cong_G \frac{U_{i-1}N_i}{N_i} = \frac{C_G(V)}{N_i} \cong_G V.$$

Therefore, $|C_G(V)/R_G(V)| = |V|^{\delta_G(V)}$, so that

$$\frac{C_G(V)}{R_G(V)} \cong_G V^{\delta_G(V)}.$$

□

From now on, we will always denote by $\delta_G(V)$ the number for which $C_G(V)/R_G(V) \cong_G V^{\delta_G(V)}$.

This theorem and Theorem 2.25 show that each chief factor between $C_G(V)$ and $R_G(V)$ is isomorphic to V as a G-module. Moreover, we can see in the following theorem that these chief factors are actually complemented.

Theorem 2.30. *Each chief factor H/K between $C_G(V)$ and $R_G(V)$ is complemented in G/K.*

Proof. Using the notation of the proof of Theorem 2.29, we will prove that for every $1 \leq i \leq \delta_G(V)$, the quotient $U_{i-1}/U_i \cong_G V$ is complemented in G/U_i. As said before, $U_{i-1}N_i = C_G(V)$, so

$$C_G(V)/N_i \cong_G U_{i-1}/U_i \cong_G V.$$

By Corollary 2.20, $C_G(V)/N_i$ is complemented in G/N_i, so let D/N_i be its complement. On the one hand,

$$U_{i-1}D = U_{i-1}DN_i = C_G(V)D = G.$$

On the other hand,

$$U_{i-1} \cap D = U_{i-1} \cap C_G(V) \cap D = U_{i-1} \cap N_i = U_i.$$

Thus, D/U_i is also a complement of U_{i-1}/U_i in G/U_i. The lemma follows by Theorem 2.25. □

Our next goal will be proving that the group $R_G(V)$ is unique and minimal satisfying the property that $C_G(V)/R_G(V)$ is complemented. We can find this result (Theorem 2.33) after the following two lemmas. The first one says that, indeed, $C_G(V)/R_G(V)$ is complemented, while the following says that there is no more complemented chief factor G-isomorphic to V over $C_G(V)$ and under $R_G(V)$.

Lemma 2.31. *The crown $C_G(V)/R_G(V)$ is complemented in $G/R_G(V)$.*

Proof. We use again the notation of the proof of Theorem 2.29. By Theorem 2.30, we know that each U_{i-1}/U_i is complemented in G/U_i for every $i \geq 1$. So, let D_1 and D_2 be the complements of $C_G(V)/U_1$ and U_1/U_2 respectively. On the one hand,

$$(D_1 \cap D_2)C_G(V) = (D_1 \cap D_2)U_1N_2$$

and by the Dedekind Law, this is equal to

$$(D_1 \cap D_2U_1)N_2 = (D_1 \cap G)N_2 = D_1N_2 = D_1U_1N_2 = D_1C_G(V) = G.$$

On the other hand,

$$(D_1 \cap D_2) \cap C_G(V) = U_1 \cap D_2 = U_2.$$

Therefore, we have proved that $D_1 \cap D_2$ is a complement of $C_G(V)/U_2$. Following the same procedure for all chief factors U_{i-1}/U_i we conclude that $C_G(V)/R_G(V)$ is complemented in $G/R_G(V)$. □

Lemma 2.32. *There is no complemented chief factor H/K of G isomorphic to V as a G-module over $C_G(V)$ or under $R_G(V)$.*

Proof. The chief factor H/K is abelian, so clearly, $H \leq C_G(H/K) = C_G(V)$.

On the other hand, assume by contradiction that there exists a complemented chief factor $H/K \cong_G V$ with $H \leq R_G(V)$. Since G is solvable, it follows that its complement must be a maximal subgroup M/K of G/K. By Lemma 2.21, we have

$$C_G(V)/M_G \cong_G H/K \cong_G V,$$

and so $M_G \in \Delta(G, V)$. This implies $H \leq R_G(V) \leq M_G \leq M$, which is a contradiction. So, $H \nleq R_G(V)$, as we wanted. □

Theorem 2.33. *The subgroup $R_G(V)$ of G coincides with the unique minimal subgroup R of G such that $C_G(V)/R$ is isomorphic as a G-module to a direct product of some copies of V and $C_G(V)/R$ is complemented in G/R.*

Proof. By Theorem 2.29 we know that $C_G(V)/R_G(V) \cong_G V^{\delta_G(V)}$ for some $\delta_G(V) \geq 0$, and by Lemma 2.31, $C_G(V)/R_G(V)$ is complemented.

Let us prove the minimality of $R_G(V)$. Assume there exists $R' \trianglelefteq G$ such that $R_G(V)/R' \cong_G V^s$ for some $s \geq 1$, and suppose $C_G(V)/R'$ is complemented in G/R'. Of course, there exists $N \trianglelefteq G$ such that $R' \leq N \leq R_G(V)$ and $R_G(V)/N \cong_G V$. Besides, since $C_G(V)/R'$ is complemented in G/R', so is $C_G(V)/N$ in G/N. Then, there exists $D \leq G$ such that $G/N \cong V^{\delta_G(V)+1} \rtimes D/N$, and so, $R_G(V)/N \cong_G V$ is complemented in G/N by $V^{\delta_G(V)} \rtimes D/N$. However, this is a contradiction by Lemma 2.32. So, we have proved the minimality.

We prove now the uniqueness. By contradiction, assume there exists a normal subgroup R' of G where $C_G(V)/R'$ is complemented and isomorphic as a G-module to some copies of V and $R_G(V) \nleq R'$. Then $R_G(V)R'$ is a normal subgroup of G lying in $C_G(V)$, and so, $R_G(V)R'/R_G(V)$ is G-isomorphic to some copies of V. Thus, there exists $N \trianglelefteq G$ such that $R' \leq N \leq R'R_G(V)$ and $R'R_G(V)/N \cong_G V$. Since $C_G(V)/R'$ is complemented in G/R', so is $C_G(V)/N$ in G/N, and using the same arguments as before, there exists a maximal subgroup M/N of G/N complementing $R'R_G(V)/N$. Besides, $M_G \in \Delta(G, V)$. Thus, $N, R_G(V) \leq M_G \leq M$, so $R'R_G(V) \leq M$, which is a contradiction. So, $R_G(V)$ is unique. □

It is now easy to prove that the number $\delta_G(V)$ of the copies of V is characterised by the following.

Theorem 2.34. *Let G be a solvable group and V a finite irreducible G-module. Then, the number $\delta_G(V)$ of copies of V for which the direct product $V^{\delta_G(V)}$ is isomorphic to the crown $C_G(V)/R_G(V)$, is precisely the number of complemented chief factors G-isomorphic to V of any chief series of G.*

Proof. It follows immediately from Theorem 2.30, Lemma 2.32 and Theorem 2.25. □

We have seen in Lemma 2.31 that the crown $C_G(V)/R_G(V)$ has a complement in $G/R_G(V)$. It would be interesting if we had a similar result for $R_G(V)$ in $C_G(V)$, that is, if we could say that $R_G(V)$ is complemented in $C_G(V)$. Even if this is not always true, the following theorem proves that if $\Phi(G) = 1$, then there exists a chief factor of G for which we can say even more. First, however, we need a lemma, which will ensure the triviality of the Frattini subgroup when working modulo $R_G(V)$.

Theorem 2.35. *The factor group $G/R_G(V)$ has trivial Frattini subgroup, that is,*

$$\Phi(G/R_G(V)) = 1.$$

Proof. Let $N/R_G(V)$ be a minimal normal subgroup of $G/R_G(V)$. If $N \leq C_G(V)$, then, by Theorem 2.30, it is complemented in $G/R_G(V)$, so $N \not\leq \Phi(G/R_G(V))$.

If $N \not\leq C_G(V)$, consider a minimal normal subgroup $M/R_G(V)$ which is contained in $C_G(V)/R_G(V)$. Of course, $N \cap M = R_G(V)$, and so, since both N and M are normal, $N \leq C_G(M/R_G(V))$. However, this is a contradiction since $M/R_G(V) \cong_G V$. Therefore, there is not any minimal normal subgroup of $G/R_G(V)$ contained in the Frattini subgroup of $G/R_G(V)$, so that $\Phi(G/R_G(V)) = 1$. □

Theorem 2.36. *Let G be a finite solvable group with $\Phi(G) = 1$. Then there exists an irreducible G-module V and a subgroup $D \neq 1$ of G such that*

$$C_G(V) = R_G(V) \times D.$$

In such a case, $D \cong_G V^{\delta_G(V)}$.

Proof. We argue by induction on the order of G. Let N be a minimal normal subgroup of G. Since $\Phi(G) = 1$, there exists a maximal subgroup K of G not containing N, and since G is solvable, $N \cap K$ is normal in both N and K. Thus, since $G = NK$, we have $N \cap K \trianglelefteq G$, so that $N \cap K = 1$, and K is a complement of N. As we have seen, N is an irreducible G-module, and by Theorem 2.34, the crown $C_G(N)/R_G(N)$ is not trivial. By Lemma 2.32 we have $N \not\leq R_G(N)$. Thus, there exists $N_0 \in \Delta(G, N)$ such that $N \not\leq N_0$, and then $C_G(N) = N \times N_0$.

If $N_0 = R_G(N)$, then the normal subgroup $D = N$ and the irreducible G-module $V = N$ fulfils our requirements.

So, we may assume that $R_G(N) < N_0$, or which is the same, $\delta_G(N) \geq 2$. Then, $R_G(N) \times N < C_G(N)$, and write $F/N := \Phi(G/N)$. It is easy to check that

$$\frac{C_G(N)/N}{R_G(N)N/N}$$

is a crown of G/N associated to N, and by Theorem 2.34, it is not trivial. By Theorem 2.35 we know that

$$\Phi(\frac{G/N}{R_G(N)N/N}) = 1,$$

so we have $F \leq R_G(N)N$. By the Dedekind Law, $F = F \cap R_G(N)N = N \times (F \cap R_G(N))$. Write $M := F \cap R_G(N)$. Assume $M \neq 1$, and let A be a minimal normal subgroup of G contained in M. Since $\Phi(G) = 1$, there exists a maximal subgroup L of G complementing A, and consider G/L_G. Note that by Lemma 2.21 we have

$$ANL_G/L_G \leq \mathrm{Soc}(G/L_G) = AL_G/L_G.$$

So, $AN = A(AN \cap L_G)$. On the one hand, $LAN = G$, and on the other hand, by the Dedekind Law,

$$L \cap AN = L \cap (A(AN \cap L_G)) = (L \cap A)(AN \cap L_G) = AN \cap L_G.$$

Thus, L complements both $AN/(AN \cap L_G)$ and A. By Theorem 2.25, all chief factors of AN are complemented, so we deduce that AN/N is complemented in G/N. However, this is a contradiction, since $AN/N \leq F/N = \Phi(G/N)$. Therefore, $F = N$, and we can apply the inductive hypothesis. Thus, there exists V an irreducible G/N-module and a subgroup $D_1/N \neq 1$ such that $C_{G/N}(V) = R_{G/N}(V) \times D_1/N$.

Suppose first that $V \cong_G N$. Then $C_{G/N}(V) = C_G(N)$ and $R_{G/N}(V) = R_G(N) \times N$. So, taking $D = D_1$ we have $C_G(N) = R_G(N) \times D_1$. Indeed, $R_G(N)D_1 = R_G(N)ND_1 = C_G(N)$ and by the Dedekind Law,

$$N = D_1 \cap R_{G/N}(V) = D_1 \cap (R_G(N) \times N) = (D_1 \cap R_G(N)) \times N,$$

so $D_1 \cap R_G(N) = 1$.

Suppose now that the chief factors of G between N and D_1 are not G-isomorphic to N. If $C_G(N)/N \leq (R_G(N)N/N)(D_1/N)$, then by the Dedekind Law, $C_G(N) = R_G(N)(C_G(N) \cap D_1)$. Then

$$C_G(N)/R_G(N) \cong_G R_G(N)(C_G(N) \cap D_1)/R_G(N) \cong_G (C_G(V) \cap D_1)/(R_G(N) \cap D_1),$$

and recall that $N \leq C_G(N) \cap D_1$. Hence all chief factors of G between $(R_G(N) \cap D_1) \times N$ and $C_G(N) \cap D_1$ are G-isomorphic to N. By assumption no chief factor of G between N and D_1 is G-isomorphic to N, so we deduce that $C_G(N) \cap D_1 = (R_G(N) \cap D_1) \times N$. Then, $C_G(N) = R_G(N)N$, which is a contradiction since we said $\delta_G(N) \geq 2$. Therefore, we assume $(R_G(N)N/N)(D_1/N) < C_G(N)/N$. Note that

$$R_G(N) \leq R_G(N)N \leq R_G(N)D_1 \leq C_G(N),$$

so every chief factor of G between $R_G(N)N$ and $R_G(N)D_1$ is G-isomorphic to N. Since

$$\begin{aligned} D_1R_G(N)/NR_G(N) &= D_1NR_G(N)/NR_G(N) \\ &\cong_G D_1/(D_1 \cap NR_G(N)) \\ &\cong_G D_1/N(D_1 \cap R_G(N)), \end{aligned}$$

and we said that all chief factors of G between M and D_1 are not G-isomorphic to N, we have $D_1 = N(D_1 \cap R_G(N))$. In this case, we take $D = D_1 \cap R_G(N) \neq 1$ and we have

$$C_{G/N}(V) = R_{G/N}(V) \times D.$$

Since the crown $C_{G/N}(V)/R_{G/N}(V)$ is not trivial, by Theorem 2.34, V must be isomorphic as a G-module to some chief factor H/K of G over N. Thus, $N \leq H \leq C_{G/N}(V)$, so actually $C_{G/N}(V) = C_G(V)$. With this observation, we are done. □

Remark 2.37. This theorem is no longer true if $\Phi(G) \neq 1$. For instance, consider the finite cyclic (and so, finite solvable) group C_{12}. Notice that $\Phi(C_{12}) = C_6 \cap C_4 = C_2 \neq 1$ and consider also its minimal normal subgroup C_2. Since C_{12} is abelian, $C_{C_{12}}(C_2) = C_{12}$, and consider the chief series

$$C_{12} \geq C_6 \geq C_3 \geq 1.$$

Since $C_6/C_3 \cong_{C_{12}} C_2$ is a Frattini chief factor, the unique non-Frattini chief factor C_{12}-isomorphic to C_2 of our chief series is C_{12}/C_6, so we have $R_{C_{12}}(C_2) = C_6$. However, the subgroups supplementing C_6 are exactly C_4 and C_{12}, which of course do not complement it. So, there is not any subgroup D such that

$$C_{C_{12}}(C_2) = R_{C_{12}}(C_2) \times D,$$

as asserted.

The following result, the last one of the chapter, will be interesting in the situation of Theorem 2.36. Indeed, the subgroups D of both statements could be taken to be the same.

Theorem 2.38. *Let D be a direct product of minimal normal subgroups of G which are isomorphic as a G-module to V. If there exists a subgroup H of G such that*

$$HD = HR_G(V) = G,$$

then $H = G$.

Proof. Suppose by contradiction that $H \neq G$, and let M be a maximal subgroup of G containing H. Clearly $MD = MR_G(V) = G$. By Lemma 2.32 $R_G(V)$ has no complemented chief factors G-isomorphic to V, so $D \cap R_G(V) \leq \Phi(G)$. Observe that

$$[M \cap D, R_G(V)] \leq [D, R_G(V)] \leq D \cap R_G(V) \leq \Phi(G),$$

which means that $(M \cap D)\Phi(G)/\Phi(G) \leq Z(G/\Phi(G))$. Therefore, $(M \cap D)\Phi(G) \trianglelefteq G$, and in the same way, $(M \cap R_G(V))\Phi(G) \trianglelefteq G$.

Set $K := (M \cap D)(M \cap R_G(V))\Phi(G)$. Note that K is normal in G, and consider $\overline{G} := G/K$. Clearly, $\overline{D} = DK/K \neq 1$ since otherwise, $D \leq K \leq M$ and $G = MD = M$. Similarly, $\overline{R_G(V)} \neq 1$. Moreover, $\overline{M} \cap \overline{D} = 1$ and $\overline{M} \cap \overline{R_G(V)} = 1$, so $\overline{M}$ is a maximal subgroup of $\overline{G}$ complementing both $\overline{D}$ and $\overline{R_G(V)}$. In particular, $\overline{D}$ and $\overline{R_G(V)}$ are both minimal normal subgroups of $\overline{G}$, and by Lemma 2.21 it follows that $\overline{D} \cong_G \overline{R_G(V)}$. Of course,

$$DK/K \cong_G D/(D \cap K) \cong_G V,$$

so

$$V \cong_G DK/K \cong_G R_G(V)K/K \cong_G R_G(V)/(R_G(V) \cap K).$$

In addition, $MR_G(V) = G$ and since $R_G(V) \cap K \leq K \leq M$, we have $M \cap R_G(V) = R_G(V) \cap K$ (otherwise $M \cap R_G(V) = R_G(V)$). So, $R_G(V)/(R_G(V) \cap K)$ is a complemented chief factor G-isomorphic to V under $R_G(V)$, which is a contradiction by Lemma 2.32. □

Chapter 3

Intersections of Maximal Subgroups in Finite Solvable Groups

We recall our main problem. For a finitely generated prosolvable group G, how faster is the growth of $c_n(G)$ with respect to that of $b_n(G)$? In Theorem 1.13, in order to prove that $b_n(G)$ was polynomially bounded, the results in Theorem 1.12 have been crucial. As said in the end of the first chapter, we will try to do an analogous for $c_n(G)$, that is, we will try to get a similar result to Theorem 1.12 when working with arbitrary intersections of maximal subgroups instead of subgroups with zero Möbius number.

When working with a finite solvable group G, we will consider almost always the crown associated to an irreducible G-module V. Moreover, we will often work modulo $R_G(V)$. For this reason, in order to analyse the intersections of maximal subgroups in finite solvable groups, the discussion we present now is fundamental.

3.1 Maximal subgroups Supplementing V^t

Let H be a finite solvable group and $G = V^t \rtimes H$ where V is a faithful irreducible H-module, so that $H^1(H, V) = 0$ (Proposition 2.19). By Proposition 2.13 we have $|H^1(H, V^t)| = |H^1(H, V)|^t = 1$, so by Theorem 2.15 the complements of V^t in G are precisely the conjugates H^v where $v \in V^t$.

We will now study the maximal subgroups of G supplementing V^t in order to see then how their intersections look like. So, let $M \leq G$ be a maximal subgroup of G supplementing V^t, that is, such that $V^t M = G$. We define $W := V^t \cap M$. Since V^t is normal in G, then so is W in M, and so, since $G = V^t M$, it follows that W is an H-submodule of V^t. In addition, since V^t is a completely reducible H-module, there exists an H-submodule U of V^t such that $V^t = W \oplus U$.

Let $H^* := M \cap HU$ (note that in general, an H-submodule of V^t is normal in G since it is normalized by both V^t and H). We will show that $M = W \rtimes H^*$. Observe that $G = V^t H = WUH$, so

$$M = M \cap WUH = M \cap W(HU),$$

and by the Dedekind Law we have

$$M = (M \cap HU)W = WH^*.$$

So, we have to prove that $W \cap H^* = 1$. For this, let us first see that $UH \cap V^t = U$. One inclusion is clear. To prove the other one, take an element of $UH \cap V^t$. This element is of the form uh with $u \in U$ and $h \in H$ and besides $uh = v$ for some $v \in V^t$. Thus, $h = u^{-1}v \in H \cap V^t = 1$, so $h = 1$ and $u = v$. This shows the assertion, and hence,

$$H^* \cap V^t = (HU \cap M) \cap V^t = M \cap (HU \cap V^t) = M \cap U,$$

which is equal to 1 since $U \leq V^t$ and $M \cap V^t \cap U = W \cap U = 1$. In particular, $W \cap H^* = 1$, so that $M = W \rtimes H^*$. We have proved even more: since $V^t \cap H^* = 1$ it follows that $V^t H^* > WH^* = M$, and since M is maximal in G we have $V^t H^* = G$. Therefore, as pointed before, H^* must be a conjugate of H.

Finally, observe that W is a maximal H-submodule of V^t since otherwise, if there were an H-submodule X such that $W < X < V$, then $XH^* > MH^* = M$ so that $XH^* = G$, which is a contradiction. Therefore, we have proved that every maximal subgroup of G supplementing V^t is of the kind WH^v with $v \in V^t$ and W a maximal H-submodule of V^t.

Moreover every subgroup of this form is maximal in G: let $W'H^{v'}$ be a subgroup of G, with W' a maximal H-submodule of V^t and $v' \in V^t$. Let WH^v be a maximal subgroup of G supplementing V^t, with W a maximal H-submodule of V^t and $v \in V^t$, such that $W'H^{v'} \leq WH^v$ (notice that it exists since actually $W'H^{v'}$ supplements V^t). As seen before $V^t \cap WH^v$ is an H-submodule of V^t, and then, since $W, W' \leq V^t \cap WH^v < V^t$, we have $W = W'$. So, $W'H^{v'} = WH^{v'} \leq WH^v$, and since the order of both subgroups is the same, they must be equal. Hence, *a subgroup M of G is maximal in G supplementing V^t if and only if $M = WH^v$ with W a maximal H-submodule of V^t and $v \in V^t$*, thereby achieving a complete description of the maximal subgroups of G supplementing V^t.

3.2 Intersections of Maximal Subgroups Supplementing V^t

We follow with the notation of the previous section. Characterising the maximal subgroups of G supplementing V^t will allow us to study the intersections of maximal subgroups supplementing V^t. In fact, it allows us to prove the following theorem, which shows how these intersections look like. The proof of the theorem is divided in two cases, both being constructive. Therefore, it is convenient to read them thoroughly since they will be used later.

Lemma 3.1. *In the situation above, assume $M_1, \ldots, M_r$ are maximal subgroups of G supplementing V^t. Then*

$$\bigcap_{i=1}^{r} M_i = W \rtimes C,$$

where W is an intersection of maximal H-submodules of V^t and $C \leq H^v$ for a suitable $v \in V^t$.

Proof. We proceed by induction on r. The case $r = 1$ is already proved in the discussion above, so it suffices to study the intersection $K_1 \cap K_2$ with $K_1 = W_1 \rtimes C$, where W_1 is an intersection of maximal H-submodules of V^t and $C \leq H^{v_1}, v_1 \in V^t$ and $K_2 = W_2 \rtimes H^{v_2}$, where $W_2 \leq_H V^t$ is maximal in V^t and $v_2 \in V^t$. We distinguish two cases in turn: $W_1 + W_2 = V^t$ and $W_1 \leq W_2$ (note that there are not more cases since W_2 is maximal in V^t).

Assume $W_1 + W_2 = V^t$. In particular, there exist $w_1 \in W_1$ and $w_2 \in W_2$ such that $v_1 - v_2 = w_2 - w_1$, or equivalently, $v_1 + w_1 = v_2 + w_2$. We define $C^* := C^{w_1}$ and $H^* := H^{v_2+w_2}$. Thus, we have

$$C^* = C^{w_1} \leq (H^{v_1})^{w_1} = H^{v_1+w_1} = H^{v_2+w_2} = H^*.$$

Obviously, $W_1C = W_1C^{w_1}$ and $W_2H^{v_2} = W_2H^{v_2+w_2}$, and in general $WD = WD^w$ for every H-submodule W of V^t, every $D \leq H$ and every $w \in V^t$. In particular, we have

$$K_1 = W_1C = W_1C^{w_1} = W_1C^*$$

and

$$K_2 = W_2H^{v_2} = W_2H^{v_2+w_2} = W_2H^*.$$

Thus, let $x_1c = x_2h$ be an element of $K_1 \cap K_2$ with $x_1 \in W_1$, $c \in C^*$, $x_2 \in W_2$ and $h \in H^*$. We have $x_1 - x_2 = hc^{-1} \in V^t \cap H^* = 1$, so it follows that $x_1 = x_2$ and $h = c$. Hence, $K_1 \cap K_2 \leq (W_1 \cap W_2)C^*$, and since the other inclusion is trivial, we have the equality, as we wanted.

Assume now that $W_1 \leq W_2$. We observe that

$$K_1 \cap K_2 = W_1C \cap W_2H^{v_2} = W_1C \cap W_2C \cap W_2H^{v_2}.$$

If $W_2C \leq W_2H^{v_2}$, then

$$K_1 \cap K_2 = W_1C \cap W_2C \cap W_2H^{v_2} = W_1C \cap W_2C = W_1C = K_1$$

and we are done. So, we may assume $W_2C \not\leq W_2H^{v_2}$. This, in particular, implies $W_2H^{v_1} \neq W_2H^{v_2}$ and consequently, $v_2 - v_1 \notin W_2$ (this latter assertion follows since otherwise, $v_1 = v_2 + w_2$ for some $w_2 \in W_2$, so that we would have $W_2H^{v_1} = W_2(H^{v_2})^{w_2} = W_2H^{v_2}$).

Since V^t is completely reducible, there exists U an H-submodule of V^t such that $V^t = W_2 \oplus U$. Thus, there exists a non-trivial element $u \in U$ such that $v_2 - v_1 = w + u$ with $w \in W_2$. Hence, $H^{v_2-w} = H^{v_1+u}$ and

$$K_2 = W_2H^{v_2} = W_2H^{v_2-w} = W_2(H^{v_1})^u.$$

Let us show that $K_1 \cap K_2 = W_1C_C(u)$. Note that $C_C(u) = C_C(u)^u \leq (H^{v_1})^u$, so it is clear that $W_1C_C(u) \leq K_1 \cap K_2$. In order to prove the other inclusion let $w_1c = w_2h^u$ be an element of $K_1 \cap K_2$ with $w_1 \in W_1$, $w_2 \in W_2$, $c \in C$ and $h \in H^{v_1}$. Note that $w_1c = w_2h^u = w_2[u, h^{-1}]h$, and since H normalizes U, it follows that $[U, H] \leq U$. So, $w_1 - w_2 - [u, h^{-1}] = hc^{-1} \in V^t \cap H^{v_1} = 1$, or in other words, $w_1 - w_2 = [u, h^{-1}]$ and $h = c$. Moreover, $w_1 - w_2 = [u, h^{-1}] \in W_2 \cap U = 0$, so $w_1 = w_2$ and $[u, h^{-1}] = [u, h] = [u, c] = 0$. Therefore, $c \in C_C(u)$ and $K_1 \cap K_2 \leq W_1C_C(u)$, so that $K_1 \cap K_2 = W_1C_C(u)$, and we are done. □

Remark 3.2. In the remainder of this dissertation we will often refer to the two cases considered in the proof of this lemma as "the first case" and "the second case".

Remark 3.3. Let us focus on the last part of the proof of Lemma 3.1, where we have considered the subgroup $C_C(u)$. Since $u \in V^t$, we have $u = (v_1, \ldots, v_t)$ with $v_1, \ldots, v_t \in V$, and then, considering V as an irreducible C-module, we have $C_C(u) = \cap_{i=1}^t C_C(v_i) = C_C(\{v_1, \ldots, v_t\})$.

Recall, on the other hand, that by Remark 2.7, one can give field structure to $\mathrm{End}_C(V)$. Furthermore, since $\mathrm{End}_C(V)$ acts (with the obvious action) on V, this means that V can be seen as a $\mathrm{End}_C(V)$-vector space. Thus, if we take $\phi \in \mathrm{End}_C(V), v \in V$ and $c \in C$, then $\phi(v)^c = \phi(v)$ if and only if $\phi(v^c) = \phi(v)$, and since ϕ is invertible, this happens if and only if $c \in C_C(v)$. Returning to Lemma 3.1, since obviously $C_C(\{v_1, \ldots, v_t\}) = C_C(\langle v_1, \ldots, v_t \rangle)$, we can finally conclude that

$$C_C(u) = C_C(\langle v_1, \ldots, v_t \rangle_{\mathrm{End}_C(V)}),$$

where $\langle v_1, \ldots, v_t \rangle_{\mathrm{End}_C(V)}$ means the $\mathrm{End}_C(V)$-subspace of V generated by $v_1, \ldots, v_t$.

In view of this latter lemma, we consider families of maximal subgroups in general position supplementing V^t, say $M_1 = W_1 H^{v_1}, M_2 = W_2 H^{v_2}, \ldots, M_n = W_n H^{v_n}$, where the W_i are maximal H-submodules of V^t and $v_i \in V^t$ for every $1 \leq i \leq n$ (here, the term "general position" means that the considered family of maximal subgroups is not redundant, i.e., we need all of them to get their intersection). Set $U_j := \bigcap_{1 \leq i \leq j} W_i$. Reordering the maximal subgroups, we may assume

$$V^t > U_1 > U_2 > \ldots > U_{t^*} = \ldots = U_n = U$$

for a suitable $1 \leq t^* \leq n$.

Assume $j < t^*$. Then, since all W_i are maximal H-submodules,

$$\frac{U_j}{U_{j+1}} = \frac{U_j}{U_j \cap W_{j+1}} \cong_H \frac{U_j + W_{j+1}}{W_{j+1}} = \frac{V^t}{W_{j+1}} \cong_H V.$$

This implies that $U \cong_H V^{t-t^*}$. From our discussion of the first case in the proof of Lemma 3.1, since $U_j + W_{j+1} = V^t$ for every $1 \leq j \leq t^* - 1$ we deduce that

$$M_1 \cap \ldots \cap M_{t^*} = U \rtimes H^*$$

with H^* a suitable conjugate of H.

Let $r := n - t^*$. From the discussion of the second case in Lemma 3.1 we deduce that there exist $v_1, \ldots, v_r \in V^t$ such that

$$\bigcap_{i=1}^{n} M_i = U \rtimes C_{H^*}(\{v_1, \ldots, v_r\}).$$

Write now $v_i = (w_{i1}, \ldots, w_{it}) \in V^t$. Then we have $C_{H^*}(v_i) = \bigcap_{1 \leq j \leq t} C_{H^*}(w_{ij})$, and so, considering V as an irreducible H^*-module, we have

$$C_{H^*}(\{v_1, \ldots, v_t\}) = C_{H^*}(\{w_{ij} \mid 1 \leq i \leq r, 1 \leq j \leq t\}).$$

Finally, by Remark 3.3, V is an $\mathrm{End}_H(V)$-vector space, so we can conclude saying that

$$C_{H^*}(\{v_1, \dots, v_t\}) = C_{H^*}(Z),$$

where $Z = \langle w_{ij} \mid i \leq i \leq r, 1 \leq j \leq t\rangle_{\mathrm{End}_H(V)}$.

Intuitively, what we have done is to start with the maximal subgroup $M_1 = W_1 \rtimes H^{v_1}$ and consider first the maximal subgroups which, by the first case, decrease the order of the H-submodule on the left of the semidirect product M_1 when intersecting with it, and then consider the maximal subgroups which, by the second case, decrease the order of the subgroup on the rigth. Thus, we have proved the following theorem.

Theorem 3.4. *Let $G = V^t \rtimes H$ be a finite solvable group such that V is an irreducible H-module. Let $M_1 = W_1H^{v_1}, \dots, M_n = W_nH^{v_n}$ be maximal subgroups of G supplementing V^t, with W_i maximal H-submodules of V^t and $v_i \in V^t$ for every i. Then, we have*

$$\bigcap_{i=1}^{n} M_i = U \rtimes C_{H^*}(Z)$$

where $U = \bigcap_{i=1}^{n} W_i$, H^* is a conjugate of H and Z is an $\mathrm{End}_H(V)$-subspace of V.

Actually, we can say even more. Let $G = V^t \rtimes H$ be as in Theorem 3.4, and let $K = U \rtimes C_{H^*}(Z)$ where U is an intersection of maximal H-submodules of V^t, H^* a conjugate of H and Z an $\mathrm{End}_H(V)$-subspace of V. Consider first the maximal H-submodules $W_1, \dots, W_r$ of V^t such that its intersection equals U, and assume they are in general position. Thus, if we consider the maximal subgroups $M_1 = W_1H^*, \dots, M_r = W_rH^*$, then its intersection must be UH^*.

Let now $Z = \langle u_1, \dots, u_s\rangle_{\mathrm{End}_H(V)}$ with $u_1, \dots, u_s \in V$, and assume all u_j to be pairwise distinct for every $1 \leq j \leq s$. Consider the maximal subgroups

$$M_{r+1} = W_k(H^*)^{u_1}, \dots, M_{r+s} = W_k(H^*)^{u_s}$$

for some fixed $1 \leq k \leq r$, and let D' be an H-submodule of V^t such that $V^t \cong_H W_k \times D'$. Of course, $D' \cong_H V$, and we can then assume $Z \leq D'$, just identifying Z with an $\mathrm{End}_H(V)$-isomorphic $\mathrm{End}_H(V)$-subspace of D'. Thus, it is easy to check that

$$\bigcap_{i=1}^{s} M_i = UC_{H^*}(Z),$$

and we conclude then with the following, which is one of the main results in this paper.

Corollary 3.5. *Let $G = V^t \rtimes H$ be a finite solvable group such that V is an irreducible H-module. Then, a subgroup of G is an intersection of maximal subgroups supplementing V^t if and only if it is of the form $U \rtimes C_{H^*}(Z)$, with U an intersection of maximal H-submodules of V^t, H^* a conjugate of H and Z an $\mathrm{End}_H(V)$-subspace of V.*

In this way, we have completely described not only the maximal subgroups of G supplementing V^t, but also all their intersections. This is a very useful information. Indeed, for a general finite solvable group G and an irreducible G-module V, we always can work modulo $R_G(V)$, so that we can apply Corollay 3.5. This is exactly what we do in the next section, which gives also one of the principal theorems of this paper.

3.3 Another Approach to the Main Problem

Assume that there exists $\gamma \in \mathbb{N}$ with the property that if G is a finite solvable group, then for every V irreducible G-module G-isomorphic to a complemented chief factor of G and for every $W \leq_{\mathrm{End}_G(V)} V$ (here, $\leq_{\mathrm{End}_G(V)}$ means $\mathrm{End}_G(V)$-subspace), there exists $W^* \leq_{\mathrm{End}_G(V)} W$ such that $C_G(W) = C_G(W^*)$ and $\dim_{\mathrm{End}_G(V)}(W^*) \leq \gamma$.

Theorem 3.6. *Let G be as above and let H be an intersection of maximal subgroups of G. Then, there exists a family of maximal subgroups $M_1, \ldots, M_n$ of G such that:*

i) $H = \bigcap_{i=1}^{n} M_i$.

ii) $\prod_{i=1}^{n} |G : M_i| \leq |G : H|^{\gamma+1}$.

Proof. We proceed by induction on $|G|$. We may assume $\Phi(G) = 1$. By Theorem 2.36, we can assume there exists an irreducible G-module V such that $C = R \times D$ with $1 \neq D \cong_G V^t$, where $C = C_G(V)$, $R = R_G(V)$ and $t = \delta_G(V)$.

If $D \leq H$ we can then conclude by induction, so we assume $D \not\leq H$. We can write

$$H = X_1 \cap \ldots \cap X_\rho \cap Y_1 \cap \ldots \cap Y_\sigma,$$

being X_i maximal subgroups not containing D for $1 \leq i \leq \rho$ and Y_j maximal subgroups containing D for $1 \leq j \leq \sigma$. We define $X := \bigcap_{i=1}^{\rho} X_i$ and $Y := \cap_{j=1}^{\sigma} Y_j$.

By Theorem 2.38 we know that if any of the X_i is a subgroup of G such that $X_i R = X_i D = G$, then $X_i = G$. Hence, $R \leq X_i$ for every i, or in other words, $R \leq X$. By Lemma 2.31, there exists $K \leq G$ such that

$$G/R = DR/R \rtimes K/R \cong V^t \rtimes K/R,$$

where V can be seen as an irreducible faithful K/R-module. Note that X/R is an intersection of maximal subgroups of G/R supplementing $DR/R \cong_{K/R} V^t$, so by Lemma 3.1, there exists a subgroup K^*/R of G/R such that

$$X/R = T/R \rtimes K^*/R,$$

with $T = DR \cap X$. Define $D^* = D \cap X$. Thus, by the Dedekind Law, we have $T = DR \cap X = (D \cap X)R = D^*R$, and note that

$$D^*R/R \cong_G D^*/(D^* \cap R) = D^* \leq_G V^t.$$

Since $D^* \leq_G V^t$, we have $V^t/D^* \cong V^{t^*}$ for some $1 \leq t^* \leq \rho$ (note that $t^* \neq 0$ since otherwise, $D \leq X$, which is a contradiction since the maximal subgroups X_i supplement D), and by recalling the proof of Corollary 3.5 we may assume ρ to be equal to $t^* + \gamma$. Observe that V is isomorphic to a minimal normal subgroup N/R of G/R, which is not contained in the maximal subgroups X_i/R. Since $G = DX_i$, it follows that $D \cap X_i$ is normal in G, so N/R and X_i/R are complements. Therefore, $|G : X_i| = |V|$ for every i.

On the other hand, $Y \geq D$ implies $XY \geq XD$, and so $|XY| \geq |XD|$. Hence,

$$|X||Y|/|X \cap Y| \geq |X||D|/|X \cap D|,$$

so

$$|Y : X \cap Y| \geq |D : X \cap D| = |D : D^*| = |V|^{t^*}.$$

Since $D \neq 1$, we can work by induction on the order of the group and consider G/D, so we can assume $\prod_j |G : Y_j| \leq |G : Y|^{\gamma+1}$. Hence, since $t^* \geq 1$,

$$\begin{aligned}\prod_{i=1}^{\rho} |G : X_i| \prod_{j=1}^{\sigma} |G : Y_j| &\leq |V|^{t^*+\gamma} |G : Y|^{1+\gamma}\\ &\leq (|G : Y||V|^{t^*})^{1+\gamma}\\ &\leq (|G : Y||Y : X \cap Y|)^{1+\gamma}\\ &\leq |G : X \cap Y|^{1+\gamma},\end{aligned}$$

and the theorem follows. □

We can finally prove the following theorem. As it says, we can give an affirmative answer to our main problem if we assume the hypothesis of Theorem 3.6. To prove it we follow the proof of Theorem 1.13.

Theorem 3.7. *Suppose that there exists a constant γ with the property that for every finite solvable group H, for every irreducible H-module V isomorphic as an H-module to a complemented chief factor of H, and for every $W \leq_{\mathrm{End}_H(V)} V$, there exists $W^* \leq_{\mathrm{End}_H(V)} W$ such that $C_H(W) = C_H(W^*)$ and $\dim_{\mathrm{End}_H(V)}(W^*) \leq \gamma$.*

Then, for every finitely generated prosolvable group G, there exists a constant β such that $c_n(G) \leq n^\beta$.

Proof. By Theorem 1.4 we know that G has PMSG, which means that there exists a constant α such that for each $n \in \mathbb{N}$, we have $m_n(G) \leq n^\alpha$. Now, for $n \neq 1$, we want to count the number of subgroups H with $|G : H| = n$ which are intersections of maximal subgroups. Fix such an $H \leq G$, and by Theorem 3.6 we can consider a family of maximal subgroups $M_1, \ldots, M_t$ such that $H = \cap_{1 \leq i \leq t} M_i$ and $n_1 \ldots n_t \leq n^{\gamma+1}$, where $n_i = |G : M_i|$. There are at most

$$1 + 2 + \ldots + n^{\gamma+1} = \frac{n^{\gamma+1}(n^{\gamma+1}+1)}{2}$$

possible factorizations of numbers $\leq n^{\gamma+1}$ (see [14]), and for each fixed factorization $n_1 \ldots n_t$, there are at most n_i^α choices for the maximal subgroup M_i corresponding to n_i. Therefore, there are at most $n_1^\alpha \ldots n_t^\alpha \leq n^{(\gamma+1)\alpha}$ choices for the family $M_1, \ldots, M_t$, and we conclude that

$$b_n(G) \leq \frac{n^{\gamma+1}(n^{\gamma+1}+1)}{2} n^{(\gamma+1)\alpha}.$$

Obviously, we always can find a constant β such that

$$\frac{n^{\gamma+1}(n^{\gamma+1}+1)}{2} n^{(\gamma+1)\alpha} \leq n^\beta,$$

for any $n \geq 1$, so the proof is complete. □

Therefore, the main problem of this paper is reduced (as said in the introduction) to the following one.

Conjecture 2. Does there exist a constant γ with the following property? If G is a finite solvable group, V an irreducible G-module and $W \leq_{\mathrm{End}_G(V)} V$, then W contains an $\mathrm{End}_G(V)$-subspace W^* such that:

i) $\dim_{\mathrm{End}_G(V)}(W^*) \leq \gamma$.

ii) $C_G(W) = C_G(W^*)$.

Chapter 4

Special Cases

In this final chapter we will give some examples in which Conjecture 2 can be answered in an affirmative way. In particular, in these examples we will be able to conclude that if we consider an inverse limit of such groups then we get profinite groups such that $c_n(G)$ is polynomially bounded.

4.1 The Supersolvable Case

It is not difficult to prove that we can find the constant γ we are looking for when G is a finite supersolvable group. Recall that G is supersolvable if there exists a normal cyclic series, that is, a normal series

$$1 = N_0 < N_1 < \ldots < N_r = G,$$

for some $r \in \mathbb{N}$ such that each factor N_i/N_{i+1} is cyclic.

In such a case, since all subgroups of a cyclic group are characteristic in it, then they are normal in the whole group, and since a cyclic group has one subgroup for each divisor of the order of the group, it follows that all chief series of G are of the form

$$1 = H_0 < H_1 < \ldots < H_s = G$$

for some $s \in \mathbb{N}$, with $H_i \trianglelefteq G$ and $|H_i/H_{i+1}| = p_i$ for some prime p_i.

Thus, if V is an irreducible G-module G-isomorphic to some chief factor, then $|V| = p$ for some prime p, and its $\mathrm{End}_G(V)$-subspaces are exactly V and the trivial one. This means that $\dim_{\mathrm{End}_G(V)}(V) = 1$, and choosing $\gamma = 1$, our result follows easily.

It can be deduced then the following.

Theorem 4.1. *Let G be a finitely generated prosupersolvable group. Then, there exists a constant β such that $c_n(G) \leq n^\beta$ for every $n \geq 1$. In other words, $\{c_n(G)\}_{n\in\mathbb{N}}$ is polynomially bounded.*

4.1.1 Intersections of Maximal Subgroups with Zero Möbius Number in Supersolvable Groups

Even if the number of intersections of the maximal subgroups in a finitely generated pro-supersolvable group G grows polynomially with respect to the index, it may happen that the amount of such subgroups is really “big” comparing with the number of subgroups of G with non-zero Möbius number. That is, even if both $b_n(G)$ and $c_n(G)$ are polynomially bounded, the probability for a intersection of maximal subgroups to have non-zero Möbius number is zero. Indeed, in what follows, we give an example in which this phenomenon happens.

Recall that the Dirichlet Theorem on arithmetic progressions states that for any two positive coprime integers a and b, there exist infinitely many primes which are congruent to a modulo b, that is, there are infinitely many primes of the form $a + rb$, where $r \in \mathbb{N}$. In particular, the arithmetic progression

$$\{1 + r2^n \mid r \in \mathbb{N}\}$$

contains infinitely many primes, for every $n \geq 1$. This implies that there exists an strictly ascending sequence $\{p_n\}_{n\in\mathbb{N}}$ of primes with the property that 2^n divides $p_n - 1$.

Let V_m be a 1-dimensional vector space over $\mathbb{F}_m$, where $\mathbb{F}_m$ is the field of p_m elements. Let also $H_n := \langle x_n \rangle$ be a cyclic group of order 2^n for $n \in \mathbb{N}$. We can define an action of H_n on V_m, for every $m \leq n$, as follows: if $v \in V_m$, then $v^{x_n} := \zeta_m v$, where ζ_m is an element of order 2^m in $\mathbb{F}_m^*$ (recall that 2^m divides $p_m - 1$). This action is well defined, since $m \leq n$ implies $\zeta_m^{2^n} = (\zeta_m^{2^m})^{2^{n-m}} = 1$, and so

$$v^1 = v^{x_n^{2^n}} = \zeta_m^{2^n} v = v.$$

In addition, note that $C_{H_n}(V_m) = \langle x_n^{2^m} \rangle$.

Knowing this, we construct the group

$$G_n = (V_1 \times \ldots \times V_n) \rtimes H_n.$$

This group is obviously supersolvable, and note that each V_i is an irreducible H_n-module, so that $V_1 \times \ldots \times V_n$ is a completely reducible H_n-module.

Let us consider its maximal subgroups. If a maximal subgroup M of G_n contains $V_1 \times \ldots \times V_n$, then it corresponds to a subgroup of $G_n/(V_1 \times \ldots \times V_n) \cong H_n$. Since H_n has a unique maximal subgroup, we then conclude that there exists a unique maximal subgroup of G_n containing $V_1 \times \ldots \times V_n$, that is $M = (V_1 \times \ldots \times V_n) \rtimes \langle x_n^2 \rangle$. Observe that this maximal subgroup has index 2.

On the other hand, assume that M is a maximal subgroup of G_n supplementing $V_1 \times \ldots \times V_n$. Since G_n is supersolvable, all its maximal subgroups have prime index, and so, $|G_n : M|$ must be p_i for some $1 \leq i \leq n$. Since $|G_n| = p_1 \ldots p_n 2^n$, it follows that all maximal subgroups supplementing $V_1 \times \ldots \times V_n$ are Hall-subgroups, and so, the maximal subgroups of the same index are all conjugate. Write

$$W_i := V_1 \times \ldots \times V_{i-1} \times V_{i+1} \times \ldots \times V_n.$$

Obviously, the subgroup W_iH_n is maximal in G_n with index p_i, and so, we can deduce that the maximal subgroups of G_n supplementing $V_1 \times \ldots \times V_n$ are exactly $W_iH_n^v$, with $v \in V_i$. Note that in this case, we have p_i maximal subgroups of index p_i for every $1 \leq i \leq n$.

Consider now the maximal subgroups $M_1 = W_i \rtimes H_n^{v_1}$ and $M_2 := W_i \rtimes H_n^{v_2}$ with $v_1, v_2 \in V_i$. If $v_1 \neq v_2$, then $M_1 \neq M_2$ (since otherwise $v_1v_2^{-1} \in N_G(W_iH_n) = W_iH_n$) , and by the second case of Lemma 3.1, we get $M_1 \cap M_2 = W_i \rtimes \langle x^{2^i} \rangle^{v_3}$ with $v_3 \in V_i$. Observe that this is a subgroup of index p_i2^i.

As we have seen in Theorem 1.12, if K is a subgroup of G with $\mu_{G_n}(K) \neq 0$, then there exists a family of maximal subgroups $M_1, \ldots, M_t$ of G_n such that $K = M_1 \cap \ldots \cap M_t$ and $|G_n : K| = |G_n : M_1| \ldots |G_n : M_t|$. Observing the intersection of maximal subgroups we have just computed, it follows that the indices of the maximal subgroups whose intersection equals K must be pairwise distinct. In other words, the indices $|G_n : M_i|$ are pairwise distinct. Therefore, keeping in mind the first and the second case of the proof of Theorem 3.1, it follows that there exists $J \subseteq \{1, \ldots, n\}$ such that K is equal to a suitable conjugate of either

$$\prod_{j \notin J} V_j \rtimes H \quad \text{or} \quad \prod_{j \notin J} V_j \rtimes \langle x^2 \rangle,$$

with indices $\prod_{j \in J} p_j$ and $2 \prod_{j \in J} p_j$ respectively. However, as we have seen, we may obtain as intersection of maximal subgroups something like

$$\prod_{j \notin J} W_j \rtimes \langle x^{2^i} \rangle$$

for every $i \in J$ with index $2^i \prod_{j \in J} p_j$. Therefore, we have proved that if $b(G)$ is the number of subgroups of G with non-zero Möbius number and $c(G)$ is the number of subgroups which are intersections of maximal subgroups, then $b(G)/c(G) \leq 1/n$. In other words, the probability for an intersection of maximal subgroups to have non-zero Möbius number is less than $1/n$.

Note that if we consider G_n and G_{n+1}, we can then define a map $\varphi_{n,n+1} : G_{n+1} \to G_n$ by sending $(v_1, \ldots, v_{n+1})x_{n+1}^i$ to $(v_1, \ldots, v_n)x_n^i$. It is easy to check that these $\varphi_{n,n+1}$ are all homomorphism of groups, and we could consider the inverse limit

$$\varprojlim_n G_n$$

with them. Thus, one can check that in this new prosolvable group, the probability for an intersection of maximal subgroups to have non-zero Möbius number is

$$\lim_{n \to \infty} \frac{1}{n} = 0.$$

4.2 A More General Case

We will consider now a more general case than the supersolvable one. Indeed, we will consider the case in which G is a finite group such that G' is nilpotent. Note that since

G/G' is abelian and G' is nilpotent, then such a group must be solvable. We can see in the following proposition why it is actually a more general case than the supersolvable case.

Proposition 4.2. *Let G be a finite supersolvable group. Then, G' is nilpotent.*

Proof. Consider a normal cyclic series

$$1 \leq N_0 < N_1 < \ldots < N_{r-1} < N_r = G.$$

Let us denote $C := \cap_{i=1}^{r} C_G(N_i/N_{i-1})$. Observe that C is normal in G, so $[C \cap N_i, C] \leq C \cap N_{i-1}$ for every i. Therefore, the $C \cap N_i$ form a central series of C reaching 1, so C is nilpotent. Thus, $C \leq F(G)$. Let us see that $G' \leq C$. Since N_i/N_{i-1} is finite cyclic for every i, then $\mathrm{Aut}(N_i/N_{i-1}) \cong (\mathbb{Z}/|N_i/N_{i-1}|\mathbb{Z})^*$, so $\mathrm{Aut}(N_i/N_{i-1})$ is abelian. Therefore, each $G/C_G(N_i/N_{i-1})$ is abelian, and $G' \leq C_G(N_i/N_{i-1})$ for every i. Thus, $G' \leq \cap_{i=1}^{r} C_G(N_i/N_{i-1}) = C$, as we wanted. □

So, let G be a group such that G' is nilpotent. Equivalently, G' is contained in the Fitting subgroup $F(G)$. Let us analyse this subgroup more closely.

Lemma 4.3. *Let G be a finite solvable group. Then $F(G)/\Phi(G)$ is a direct product of complemented minimal normal subgroups of $G/\Phi(G)$.*

Proof. We can assume $\Phi(G) = 1$. Since $F(G)$ is nilpotent, it is the direct product of its Sylow subgroups. Note that these Sylow subgroups are normal in G, so that their respective Frattini subgroup is contained in the Frattini subgroup of G. Thus, they have trivial Frattini subgroup and hence, each Sylow subgroup of $F(G)$ is elementary abelian. Therefore, $F(G)$ is a direct product of elementary abelian groups, and then abelian.

Let now N be a minimal normal subgroup of G contained in $F(G)$. Since $\Phi(G) = 1$, then there exists a maximal subgroup M of G such that $G = NM$. Consider $M \cap N$. Since N is normal in G, so is $N \cap M$ is M, and since N is abelian, $N \cap M$ is normal in N. This means that $N \cap M$ is normal in G, and since N was minimal, it follows that $N \cap M = 1$. Thus, N is complemented in G by M.

Consider now $M \cap F(G)$. By the Dedekind Law we have

$$N(M \cap F(G)) = NM \cap F(G) = G \cap F(G) = F(G),$$

and since obviously $N \cap (M \cap F(G)) = 1$, it follows that $M \cap F(G)$ complements N in $F(G)$. In addition, since $F(G)$ is normal in G, so is $M \cap F(G)$ in M, and since $F(G)$ is abelian, then $M \cap F(G)$ is also normal in $F(G)$. Therefore, $M \cap F(G)$ is normal in $G = F(G)M$. Repeating the same argument with $F(G) \cap M$ instead of $F(G)$, and following until we reach 1, we can conclude with the desired result. □

We will see now that $F(G)/\Phi(G)$ is not only a direct product of complemented minimal normal subgroups of $G/\Phi(G)$, but it is also complemented in the finite solvable group G. It is, in fact, an immediate corollary of the following lemma.

Lemma 4.4. *Let G be a finite group with trivial Frattini subgroup, and let N be an abelian normal subgroup of G. Then, N is complemented.*

Proof. Let us consider the family

$$\{M \leq G \mid NM = G\}.$$

Since $\Phi(G) = 1$, this family is not empty, and choose a minimal M from it. Consider the subgroup $N \cap M$. Of course, it is normal in N since N is abelian, and since N is normal in G, then $N \cap M$ is normal in M. Thus, $N \cap M$ is normal in $G = NM$. By contradiction, assume $N \cap M \neq 1$. If $N \cap M \leq \Phi(M)$, then, by Lemma 2.22 we have $N \cap M \leq \Phi(G) = 1$, so we may assume $N \cap M \not\leq \Phi(M)$. Let N' be a maximal subgroup of M such that $(N \cap M)N' = M$. Then, $G = NM = N(N \cap M)N' = NN'$, contradicting the minimality of M. □

Now that we know some properties of the groups G such that G' is nilpotent, we can conclude with Theorem 4.6 and Corollary 4.7 and 4.8 after it, which, as said, generalise the supersolvable case. Moreover, Theorem 4.6 ensures not only that in a finite group G such that $G' \leq F(G)$ we have $\dim_{\mathrm{End}_G(V)}(V) = 1$ for every G-module V isomorphic as G-modules to a complemented chief factor of G, but also the opposite result. In other words, it ensures that these two properties are equivalent. In order to prove it we first require a lemma, which gives some basic properties of the Fitting subgroup.

Lemma 4.5. *Let G be a solvable group. Then:*

i) If $1 \neq N \trianglelefteq G$, then N contains a non-trivial normal abelian subgroup of G, and $N \cap F(G) \neq 1$.

ii) $C_G(F(G)) \leq F(G)$.

Proof. Let us call $G^{(i)}$ to the terms of the derived series, and let i be the largest integer such that $G^{(i)} \cap N \neq 1$. Then, $(N \cap G^{(i)})' \leq N \cap G^{(i+1)} = 1$, so that $N \cap G^{(i)}$ is abelian and normal in G.

For part *ii*), suppose by contradiction that $C_G(F(G)) \not\leq F(G)$. By *i*), there exists $A/F(G) \trianglelefteq G/F(G)$, such that $F(G) < A \leq C_G(F(G))F(G)$ and $A/F(G)$ is abelian. Therefore, $A' \leq F(G)$. Note that by the Dedekind Law $A = A \cap C_G(F(G))F(G) = F(G)(A \cap C_G(F(G)))$, and $\gamma_3(A \cap C_G(F(G))) \leq [A', C_G(F(G))] \leq [F(G), C_G(F(G))] = 1$, which shows that $A \cap C_G(F(G))$ is nilpotent. Therefore, $A \cap C_G(F(G)) \leq F(G)$, and $A = F(G)$, which is a contradiction. □

Theorem 4.6. *Let G be a finite solvable group. Then, G' is nilpotent if and only if for every G-module V isomorphic as a G-module to a complemented chief factor of G we have* $\dim_{\mathrm{End}_G(V)}(V) = 1$.

Proof. If $\Phi(G) \neq 1$, consider a chief series passing through $\Phi(G)$ and let V be an irreducible G-module G-isomorphic to a complemented chief factor H/K of G. Note that $H \not\leq \Phi(G)$ since H/K would not be complemented. So, assume $\Phi(G) \leq K$. In this case $\Phi(G) \leq C_G(V)$, and it is equivalent to say that V is a G-module or a $G/\Phi(G)$-module. Furthermore, a subgroup of G is nilpotent if and only if so is modulo Frattini. These two observations imply that we may assume $\Phi(G) = 1$.

So, assume $\Phi(G) = 1$, and suppose first that G' is nilpotent. By Lemma 4.3 we have $F(G) = N_1 \times \ldots \times N_t$ where each N_i is an abelian minimal normal subgroup of G. Hence, $F(G)$ is abelian. By Lemma 4.4 there exists $H \leq G$ such that

$$G = F(G) \rtimes H = (N_1 \times \ldots \times N_t) \rtimes H.$$

Moreover, since $G' \leq F(G)$, it follows that $G/F(G) \cong H$ is also abelian.

Let now V be an irreducible G-module G-isomorphic to a complemented chief factor H/K of G. We consider a chief series passing through $F(G)$, and we observe that since $F(G)$ is abelian, then $F(G) \leq C_G(V)$. This means that these chief factors can be seen as $G/F(G)$-modules, and since $G/F(G) \cong H$, as H-modules.

Since H is abelian, it follows that if we define the map

$$\begin{aligned} \iota : H &\longrightarrow \mathrm{End}_H(V) \\ h &\longmapsto (v \mapsto v^h), \end{aligned}$$

then it is well defined. Indeed, for every $h' \in H$ we have

$$\iota(h)(v^{h'}) = (v^{h'})^h = v^{h'h} = v^{hh'} = (v^h)^{h'} = \iota(h)(v)^{h'}.$$

Therefore, each element of H can be viewed as an element of $\mathrm{End}_H(V)$, and since V is an irreducible H-module, it follows that nor does it have non-trivial proper $\mathrm{End}_H(V)$-subspaces. Thus, its dimension as an $\mathrm{End}_H(V)$-vector space must be 1.

Suppose now that $\dim_{\mathrm{End}_G(V)}(V) = 1$ for every G-module V isomorphic as a G-module to a complemented chief factor of G. As we have seen in Lemma 4.3, the Fitting subgroup of G is a direct product of complemented abelian minimal normal subgroups. Write again

$$F(G) = N_1 \times \ldots \times N_t,$$

and since in particular the N_i's are complemented chief factors, we have $\dim_{\mathrm{End}_G(N_i)}(N_i) = 1$ for every i. Since $F(G)$ is abelian, Lemma 4.5 shows that actually $F(G) = C_G(F(G))$. The procedure we will follow now is similar to that of Proposition 4.2. Since $F(G)$ is a direct product of the N_i's, then $F(G) = C_G(F(G)) = \cap_{i1}^t C_G(N_i)$. On the other hand, it is easy to see that $G/C_G(N_i)$ is isomorphic to a subgrouup of $\mathrm{GL}_{\mathrm{End}_G(N_i)}(N_i)$, and since in our case $\dim_{\mathrm{End}_G(N_i)}(N_i) = 1$, it follows that

$$\mathrm{GL}_{\mathrm{End}_G(N_i)}(N_i) = \mathrm{End}_G(N_i)^*.$$

In particular, $G/C_G(N_i)$ is abelian, so that $G' \leq C_G(N_i)$ for every i. We conclude that

$$F(G) = C_G(F(G)) = \bigcap_{i=1}^{t} C_G(N_i) \leq G',$$

as desired. □

As this theorem says, we can not find a group such that the pointed dimensions are 1 and G' is not nilpotent. Now, as expected, we end with the following two corollaries.

Corollary 4.7. *Let G be a finite group such that G' is nilpotent. Then, for every subgroup H which is an intersection of maximal subgroups, there exists a family of maximal subgroups $M_1, \ldots, M_t$ satisfying:*

i) $H = M_1 \cap \ldots \cap M_t$.

ii) $|G : M_1| \ldots |G : M_t| \leq |G : H|^2$.

Proof. We are working with maximal subgroups, so we may assume $\Phi(G) = 1$. It follows then immediately from Theorem 4.6 and Theorem 3.6. □

Corollary 4.8. *Let G be a finitely generated prosolvable group with pronilpotent derived subgroup. Then, there exits a constant β such that $c_n(G) \leq n^\beta$ for every $n \geq 1$.*

Proof. By the proof of Theorem 3.7, it only remains to check that if G is an inverse limit of finite groups with nilpotent derived subgroup, then G' is pronilpotent. Let $\{N_i\}$ be a descending open normal subgroup neighbourhood basis of the identity, and consider the sections $G'N_i/N_i$. Obviously, G/N_i is a finite group with nilpotent derived subgroup, that is, $G'N_i/N_i$ is nilpotent. By Corollary 1 of [17], the derived subgroup of a finitely generated prosolvable group is closed, so one can check that

$$G' \cong \varprojlim_i G'N_i/N_i.$$

Therefore, G' must be pronilpotent. □

4.3 Base of size 3

Let G be a permutational group $G \leq \mathrm{Sym}(\Omega)$, where Ω is a set of cardinality n. A *base* for G is a sequence $\beta = (\beta_1, \ldots, \beta_r)$ from Ω with the property that only the identity of G fixes each point of β. In other words, $C_G(\beta) = 1$.

Let us denote by $\mathbb{F}_p$ the field of p elements, and by $\mathbb{F}_p^d$ the $\mathbb{F}_p$-vector space of dimension d. Seress proves in [18] (Theorem 2.1 and Theorem 3.1) the following.

Theorem 4.9. *If G is a solvable irreducible linear group acting on $\mathbb{F}_p^d$, then it has a base of size at most 3. In other words, there exist $v_1, v_2, v_3 \in \mathbb{F}_p^d$ such that $C_G(\{v_1, v_2, v_3\}) = 1$.*

As we know, our main problem is to solve Conjecture 2. In that conjecture, the solvable group G we are considering satisfies the conditions of Theorem 4.9. Even if this result does not solve Conjecture 2, we have a partial solution. Indeed, if the subspace $W \leq_{\mathrm{End}_G(V)} V$ that we consider in the conjecture is precisely the whole G-module V, then we can find, by Theorem 4.9, three elements $v_1, v_2, v_3 \in V$ such that $C_G(\{v_1, v_2, v_3\}) = 1 = C_G(V)$. Thus, considering $W^* = \langle v_1, v_2, v_3 \rangle_{\mathrm{End}_G(V)}$ we can conclude with $\gamma = 3$.

The proof of Theorem 4.9, which, as said, is in [18], is not easy at all. This can give an idea of how complicated could be solving Conjecture 2 not only for V, but for all $\mathrm{End}_G(V)$-subspaces of V.

Bibliography

[1] M. Aschbacher, R. Guralnick. Some Applications of the First Cohomology Group. *Journal of Algebra* **90** (1984), 446-460.

[2] A. Ballester-Bolincher, L. M. Ezquerro. Classes of Finite Groups. *Springer*, 2006.

[3] E. Detomi, A. Lucchini. Crowns and Factorization of the Probabilistic Zeta-Function. *Journal of Algebra* **265** (2003), 651–668.

[4] K. Doerk, T. Hawkes. Finite Soluble Groups. *Walter de Gruyter*, 1992.

[5] W. Gaschütz. Lezioni Sulla Coomologia Dei Gruppi Finiti. *Istituto di Algebra e Geometria dell'Università di Padova*, 1973.

[6] W. Gaschütz. Praefrattinigruppen. *Arch. Math.* **13** (1962), 418–426.

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

[8] B. Huppert. Endliche Gruppen I. *Springer*, 1967.

[9] A. Lubotzky, D. Segal. Subgroup Growth. *Springer*, 2003.

[10] A. Lucchini. Subgroups of Solvable Groups with Non-Zero Möbius Function. *J. Group Theory* **10** (2007), 633-639.

[11] A. Lucchini. The X-Dirichlet Polynomial of a Finite Group. *J. Group Theory* **8** (2005), 171-188.

[12] A. Mann. A Probabilistic Zeta Function for Arithmetic groups. *Internat. J. Algebra Comput.* **15** (2005), 1053-1059.

[13] A. Mann. Positively Finitely Generated Groups. *Forum Math.* **8** (1996), 429-459.

[14] L. E. Mattics and F. W. Dodd. A Bound for the Number of Multiplicative Partitions. *Amer. Math. Monthly* **93** (1986), 125-126.

[15] L. Pyber. Enumerating Finite Groups of Given Order. *Ann. Math.* **137** (1993), 203-220.

[16] D. J. S. Robinson. A Course in the Theory of Groups. *Springer*, 1996.

[17] D. Segal. Closed Subgroups of Profinite Groups. *J. London Math. Soc.* **81** (2000), 29-54.

[18] A. Seress. The Minimal Base Size of Primitive Permutation Groups. *J. London Math. Soc.* **53** (1996), 243–255.

[19] T. Wolf. Solvable and Nilpotent Subgroups of $\mathrm{GL}(n, q^m)$. *Can. J. Math.* **34** (1982), 1097-1111.