SCUOLA DI DOTTORATO
UNIVERSITÀ DEGLI STUDI DI MILANO-BICOCCA

Dipartimento di
MATEMATICA E APPLICAZIONI

Dottorato di Ricerca in MATEMATICA

Ciclo XXXIV

Curriculum in ALGEBRA E GEOMETRIA

Some questions about the Möbius function of finite linear groups

Cognome: DI GRAVINA

Nome: LUCA MARIA

Matricola: 779563

Relatrice: Prof.ssa FRANCESCA DALLA VOLTA

Coordinatore: Prof. PIERLUIGI COLLI

ANNO ACCADEMICO 2020/2021

Some questions about the Möbius function of finite linear groups

Luca Maria Di Gravina

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Mathematics

Joint PhD Program in Mathematics
Milano-Bicocca – Pavia – INdAM

Ciclo XXXIV

Supervisor: Prof. Francesca Dalla Volta

Dipartimento di Matematica e Applicazioni
Università degli Studi di Milano-Bicocca

31 January 2022

Preface

This thesis is the result of my research during the three years of my doctoral studies. It is a work that represents the attempt and effort to grow up not only as a student, but also as a researcher in mathematics. During the days of intense scientific meditations and in the sleepless nights spent on writing, it may have seemed that everything in a PhD is reduced to that. Nevertheless, I think that a thesis can not reflect the full experience of my PhD. This is not only because a PhD program consists of many different activities, which force PhD students to put their heads out of their specific research problem and broaden their mathematical horizons. But also because the doctorate is a synthesis of the thesis (and what the thesis itself represents) with an antithetical side, which has particularly had a great relevance in my case. Therefore, I want to spend a few words here below on *my antithesis*, since it will, of course, have to remain hidden later.

During my research activity, there were moments when a break from the concentration on mathematical problems was necessary. Those moments occurred in the working time and at the working place, but they were in contrast with the work itself. For this reason I call them "the antithesis" of my PhD thesis, since in those moments the thesis surely made no progress. It is funny to say, but in my case these frequent interruptions marked the natural rhythm of my hours at university. Sometimes it was just to take a look out of the window, but on many other occasions the antithesis was represented by some colleagues who needed a break and wanted to share this need with me in some office, or in a sunny courtyard, or simply in front of a coffee machine. Examples of small rituals that made the atmosphere familiar and relaxing. Probably, the existence of such nice people at the working place is not obvious, but I was very lucky and because of them I never felt like a lonely researcher in an empty space, during all my PhD. Moreover, not only did I meet a lot of good colleagues, but in many cases they turned out to be some of the loveliest people I have ever known. Mentioning singularly everyone here and listing each moment spent together is a stylistic exercise that I prefer to avoid. But I want to make it clear that for me it was difficult to imagine that I would have met so many fantastic people whom I am very happy to call my friends. And such a spirit of friendship is something that now I immediately associate with mathematics. I do not know whether it corresponds only to my personal experience, but it is always important to remember this feeling and to hope that it will never be lost. I look forward to finding a confirmation in the prefaces to future theses.

Some acknowledgements for the thesis

My most sincere gratitude goes to Francesca Dalla Volta, for having generously accepted to be my supervisor and for her dedication to such a delicate role. I always received her constant support, her advice, and encouragement, even when working remotely (and sometimes during the weekend) was inevitable. The fruitful discussions, her prudence and her constructive reprimands allowed me to understand my mistakes, not only with regard to general ideas and special arguments in the proof of mathematical problems, but also as regards the way mathematics should be explained in a thesis. Her guidance was something invaluable that I can not forget.

I wish to thank Benjamin Klopsch for his careful supervision during my period in Düsseldorf, even in the worst circumstances because of the pandemic emergency. His presence when needed, together with his interest in my work, always gave me confidence to be an active part in his research group. I really think that it is always a pleasure and a great motivation to meet someone with such a talent for mathematics and such a strong spirit of sharing knowledge.

I am obliged to Andrea Lucchini and Johannes Siemons for their reports on this thesis. Their comments and corrections were very precious.

Thanks also to Pierluigi Colli and Thomas Weigel, the coordinators of the joint PhD program that involves University of Milano-Bicocca, University of Pavia and INdAM. Their relationship with students and the attention paid to several issues are merits which go beyond their formal role. Clearly, thanks also to the institutes engaged in the mentioned successful PhD program and to all people they represent.

Finally, I want to thank all researchers and friends with whom I discussed my ideas, my work, and a lot of questions.

Luca

Contents

Chapter 1

Introduction

In the theory of partially ordered sets, the Möbius function of a locally finite poset is a generalization of the number-theoretic Möbius function. In the twentieth century, the study of its properties became an active research area in combinatorics (for instance, see [16] and [36]). Now, the Möbius function is indeed a classical tool in enumerative combinatorics, with several applications also in group theory, from the Euler characteristic of subgroup complexes to algebraic aspects of cellular automata.

For a locally finite poset $(P, \leq)$, the Möbius function is the map

$$\mu_P : P \times P \to \mathbb{Z}$$

satisfying $\mu_P(a, b) = 0$ unless $a \leq b$, and defined recursively for $a \leq b$ by

$$\mu_P(a, a) = 1 \quad \text{and} \quad \sum_{a \leq c \leq b} \mu_P(a, c) = 0 \text{ if } a < b.$$

If we have a finite lattice $(L, \leq)$ with minimum $\hat{0}$ and maximum $\hat{1}$, then $\mu_L(\hat{0}, \hat{1})$ coincides with the reduced Euler characteristic of the simplicial complex K induced by L. In particular, $\mu_L(\hat{0}, \hat{1}) = 0$ if the complex K is contractible. Other characterizations of $\mu_L(\hat{0}, \hat{1})$ can be provided, for example by using the Lefschetz character $\Lambda_{L,G}$ for the action of a group G on the lattice L (see [40] for an overview).

In this thesis, we look at the Möbius function as an interface of combinatorial questions between the theory of finite classical groups and the theory of lattices and posets that are somehow connected to these groups. Some emphasis is on the linear group $\mathrm{GL}(n, q)$, its subgroups, and relative quotients, such as the finite almost-simple groups $\mathrm{PGL}(n, q)$ and $\mathrm{PSL}(n, q)$.

An intriguing motivation for the study of the Möbius function of subgroup lattices can be found in the context of finitely generated profinite groups. If G is a finitely generated profinite group, there is a connection between the probabilistic zeta function of G and the corresponding Möbius function

$\mu : \mathcal{L}(G)_o \times \mathcal{L}(G)_o \to \mathbb{Z}$ defined on the lattice $\mathcal{L}(G)_o$ of the open subgroups of G. More precisely, we can use μ to express as

$$P(G,k) = \sum_{H \leq_o G} \frac{\mu(H,G)}{|G:H|^k}$$

the probability that k random elements of G generate the whole group.

For $s \in \mathbb{C}$, we obtain the following Dirichlet series

$$P_G(s) = \sum_{H \leq_o G} \frac{\mu(H,G)}{|G:H|^s},$$

that interpolates $P(G,k)$ in the positive integers. The convergence of $P_G(s)$ in some right half-plane of the complex plane has been studied for profinite groups that are positively finitely generated (PFG), i.e. profinite groups G such that $P(G,k) > 0$ for some k. If G is PFG, some questions arise about the growth of $|\mu(H,G)|$ and the growth of the number of subgroups $H \leq_o G$ with $\mu(H,G) \neq 0$.

Let $b_n(G)$ be the number of open subgroups $H \leq_o G$ such that the index $|G:H| = n$ and $\mu(H,G) \neq 0$. It was conjectured by Mann (see [28]) that $b_n(G)$ grows polynomially with respect to n and that $|\mu(H,G)| \leq |G:H|^c$ for some constant c independent of $H \leq_o G$. If this conjecture is true, then we get the absolute convergence of the series $P_G(s)$.

In [26], Lucchini proved that Mann's conjecture is true if we are able to solve the following similar problem concerning only finite almost-simple groups.

Conjecture. *There exist two absolute constants c_1, c_2 such that for each finite almost-simple group G we have*

(i) $|\mu(K,G)| \leq |G:K|^{c_1}$ *for all* $K \leq G$;

(ii) $b_n(G) \leq n^{c_2}$ *for all* $n \in \mathbb{N}$.

In [10], Colombo and Lucchini proved that the alternating and symmetric groups (Alt(n), Sym(n), for $n \geq 5$) satisfy this conjecture, so that they obtained a proof of Mann's conjecture for finitely generated profinite groups with the property that all the non-abelian composition factors of every finite epimorphic image are permutation groups of alternating type.

We begin to concentrate our attention on finite classical groups, particularly on general linear groups, following some methods that Shareshian studied in [38] to compute the Möbius number $\mu(1,G)$ for some classical group G. Aschbacher's classification of their maximal subgroups is important to connect the structure of the subgroup lattice of G to order structures induced by the geometry of vector spaces on which the group G acts.

Main results of the thesis

In this thesis, we study the Möbius function $\mu(H, G)$ of a finite classical group G with respect to subgroups $H \leq G$, starting from the methods that Shareshian used for $\mu(1, G)$ in his thesis ([38]). Our results usually refer to the finite general linear group $\mathrm{GL}(n, q)$. Since the action of the group G on the subspace lattice of $\mathbb{F}_q^n$ plays the fundamental role in the proofs of theorems, the choice of $G = \mathrm{GL}(n, q)$ can be replaced with $G = \mathrm{PGL}(n, q)$, if we want to relate the same results to the Möbius function of finite almost-simple groups.

We briefly observe that Chapter 2 and Chapter 3 are devoted to state preliminary notions and facts that are used throughout the thesis. In Chapter 2, in particular, we introduce the fundamental properties of posets and lattices, with emphasis on some subspace lattices induced by elements of $\mathrm{GL}(n, q)$. We see that for many linear transformations such lattices have the precise structure of a product of chains. Chapter 3 is a detailed introduction to the Möbius function, with some questions and remarks to motivate its study on the subgroup lattice of a group.

The first notable new results are contained in Chapter 4. The main idea is to approximate $\mu(H, G)$ through a *good function* $f(H, G)$, depending on some Aschbacher classes, so that

$$\mu(H, G) = f(H, G) + \sum_{K \in \mathcal{A}} \mu(H, K)$$

where $\mathcal{A}$ denotes the union of the other classes, which might be more difficult to deal with.

In particular, if $\mathcal{I}_1(G, H)$ denotes the order ideal generated by the maximal subgroups in the first Aschbacher class, that is the ordered set of all reducible subgroups of G containing H, we can use the Möbius function of

$$\widehat{\mathcal{I}}_1(G, H) = \mathcal{I}_1(G, H) \cup \{H, G\} \tag{1.1}$$

(i.e., where the minimum H and the maximum G are adjoined, *if necessary*) as the function f above. We obtain that

$$\mu(H, G) = \mu_{\widehat{\mathcal{I}}_1(G,H)}(H, G) - \sum_{\substack{K \notin \mathcal{I}_1(G,H) \\ H < K < G}} \mu(H, K)\,.$$

So, first of all, we concentrate on the term

$$\mu_{\widehat{\mathcal{I}}_1(G,H)}(H, G)$$

and we compute it in the following way.

Theorem (4.2.4).

$$-\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G) = \sum_{E \in \Psi'(G,H)} (-1)^{|E|}\,. \tag{1.2}$$

where the set

$$\Psi'(G,H) = \{E \subseteq \mathcal{S}(V,H) \setminus \{0,V\} \mid \bigcap_{W \in E} \mathrm{stab}_G(W) \neq H\}$$

depends on the lattice $\mathcal{S}(V,H)$ of H-invariant subspaces of V, and on the action of G on the subspace lattice of V.

The exact value of (1.2) can be found under special conditions for the lattice $\mathcal{S}(V,H)$. In particular, also by using original arguments, we study some examples and the case in which $\mathcal{S}(V,H)$ is a distributive lattice (under some conditions).

Similarly to $\mathcal{I}_1(G,H)$, for each irreducible subgroup $K \leq G$ we can consider the order ideal $\mathcal{I}_1(K,H)$ given by all reducible subgroups of K containing H. We present it in Chapter 5 and, as in (1.1), we have an extension $\widehat{\mathcal{I}}_1(K,H)$, so that we can similarly compute its Möbius number

$$-\mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K) = \sum_{E \in \Psi'(K,H)} (-1)^{|E|}\,.$$

Such a number appears in the following expression of the Möbius function of the group G.

Theorem (5.2.1).

$$\mu(H,G) = \sum_{K \in Irr_G(H)} \mu(K,G) \cdot \mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K) \tag{1.3}$$

where

$$Irr_G(H) = \{K \leq G \mid H \leq K,\ K \text{ is irreducible on } V\}.$$

According to the ideas of Colombo and Lucchini in [10], we can define a closure operator (see Definition 3.1.8)

$$\bar{\ }\colon \mathcal{L}(K) \to \mathcal{L}(K)$$

on the subgroup lattice $\mathcal{L}(K)$ of each irreducible subgroup K of G. A subgroup H is said to be closed in K if $\overline{H} = H$. Then

Proposition (5.2.3). *Let $H \leq G$ and $K \in Irr_G(H)$. If H is not closed in K, then*

$$\mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K) = 0\,.$$

This is interesting because we find a connection between the idea of Shareshian in [38] and the argument of Colombo and Lucchini in [10] for the alternating and symmetric groups on a finite set. We study (1.3) to get partial results in an attempt to prove Mann's conjecture reduced to the finite almost-simple groups $\mathrm{PGL}(n, q)$ and $\mathrm{PSL}(n, q)$. In this direction, we obtain the following result.

Theorem (5.3.3). *Let* $V \simeq \mathbb{F}_q^n$ *and* $G = \mathrm{GL}(n, q)$. *Let*

$$c_m^{prod}(G) := |\mathcal{F}_m^{prod}(G)|$$

where $\mathcal{F}_m^{prod}(G)$ *is the set of closed subgroups* H *in* G *such that* $|G : H| = m$ *and the lattice* $\mathcal{S}(V, H)$ *is isomorphic to a product of chains.*
Then there exists an absolute constant α*, independent of* n *and* q*, such that*

$$c_m^{prod}(G) \leq m^{\alpha} \quad \forall\, m \in \mathbb{N}\,.$$

The subgroups generated by cyclic matrices (and their closures) are examples of subgroups H such that $\mathcal{S}(V, H)$ is isomorphic to a product of chains. In Chapter 2, we recall that most of the matrices in $\mathrm{GL}(n, q)$ are cyclic.

Chapter 2

Preliminaries about posets

In this chapter we shall state some definitions and facts about partially ordered sets that will be used throughout this thesis. We begin by briefly recalling some general information about posets and by fixing the notation. Although most of the basic notions are well-known, we think that it is important to be careful and to avoid confusion for those ambiguous terms which are sometimes used with different meanings by different authors.

Afterwards, we focus on lattices, which constitute a special class of posets, and we consider some of their abstract properties. Moreover, concrete examples are presented, especially for the subspace lattice $\mathcal{S}_V$ of a vector space V. These examples are also useful to introduce the section about invariant subspace lattices induced by subgroups of $\mathrm{GL}(V)$.

Main references are [41] for §2.1, [4] for §2.2, and [18] for §2.3.

2.1 Basic notions

A *partially ordered set*, or just simply called a **poset**, is a pair $(P, \leq)$, where P is a set and $\leq$ is a partial order relation on P. It means that P is endowed with a binary relation $\leq$ that is reflexive, anti-symmetric, and transitive.

Notation. We often refer to the poset $(P, \leq)$ only by indicating the set P. If $x, y \in P$ are two elements of the poset, we use the obvious notation $x \leq y$ to mean that x is related to y, and the expression $y \geq x$ is equivalent to $x \leq y$. Moreover, we can write $x < y$ to mean that $x \leq y$ and $x \neq y$. The expression $y > x$ is equivalent to $x < y$.

Two elements x, y in a poset P are **comparable** if $x \leq y$ or $y \leq x$ holds. Otherwise, if neither $x \leq y$ nor $y \leq x$ holds, they are said to be **incomparable**. If x and y are comparable for all $x, y \in P$, then P is a **chain**, or equivalently a *totally* (or *linearly*) *ordered set.*

Definition 2.1.1. An **induced subposet** $(Q, \leq_Q)$ of a poset $(P, \leq_P)$ is a subset $Q \subseteq P$ together with a partial order relation $\leq_Q$ such that for all

$x, y \in Q$

$$x \leq_Q y \text{ in } Q \quad \Leftrightarrow \quad x \leq_P y \text{ in } P.$$

We then say that the subset Q has the ordering induced from P.

Notation. Whenever we refer to subposets, we mean induced subposets. Thus, if P is a poset and Q is a subposet of P, we use the same notation $\leq$ for both of the order relations on P and Q.

Let $(P, \leq)$ be a poset. Let $C \subseteq P$ be a subset such that the induced subposet $(C, \leq)$ is a chain. Then we say that C is a **chain in** P. The chain C is called **maximal** in P if it is not contained in a larger chain of P, i.e. if there exists no other chain C' in P such that $C \subsetneq C'$. In general, if C is a finite chain, we can define the **length** of C as

$$\ell(C) = |C| - 1\,.$$

The **length of the poset** P, denoted by $\ell(P)$, is

$$\ell(P) = \max\{\ell(C) \mid C \text{ is a chain in } P\}.$$

If there exists an infinite chain C in P, then $\ell(C) = \ell(P) = \infty$.

We say that a subset $A \subseteq P$, regarded as a subposet, is an **antichain** if for every pair of distinct elements $x, y \in A$ we have that x and y are incomparable. If $A \neq \emptyset$ is an antichain in the poset P, we can consider the set

$$P_{\leq A} = \{s \in P \mid s \leq a \text{ for some } a \in A\} \subseteq P.$$

$P_{\leq A}$ is a subposet of P and it is an *order ideal* of P, in the following sense.

Definition 2.1.2. Let $(P, \leq)$ be a poset. An **order ideal** of P (in the sense of Stanley [41]) is a subset $I \subseteq P$ such that

$$\forall\, x \in I,\ t \in P \qquad t \leq x \Rightarrow t \in I\,. \tag{2.1}$$

Clearly, I can be regarded as an induced subposet of P. We include the empty subset $\emptyset \subseteq P$ as an order ideal of P.

Notation. Some authors refer to subsets of P satisfying (2.1) as *down-sets* (see for instance [4]). For us, an order ideal is always in the sense of Stanley.

So, if $A \neq \emptyset$ is an antichain in the poset P, we say that $P_{\leq A}$ is the **order ideal of** P **generated by** A. In particular, if $A = \{x\}$, for some $x \in P$, then

$$P_{\leq x} := P_{\leq A} = \{s \in P \mid s \leq x\} \subseteq P \tag{2.2}$$

is called the **principal order ideal of** P generated by x. In this case, we also have the subposet $P_{<x} = P_{\leq x} \setminus \{x\}$.

Obviously, the antichains in P are in one-to-one correspondence with the order ideals of P generated by antichains (we consider $\emptyset \subseteq P$ as the ideal generated by the empty antichain). If P is finite, then it is also easy to see that the map $A \mapsto P_{\leq A}$ from the set of antichains to the set of all order ideals of P is surjective, and hence invertible.

Proposition 2.1.3. *Let P be a finite poset. Then there is a bijection between antichains and order ideals of P, given by the map $A \mapsto P_{\leq A}$ for all antichains A in P.*

Let $(P, \leq)$ be a poset. We recall that the **dual poset** of P is defined as the poset $(P^\sharp, \leq^\sharp)$, where the set $P^\sharp$ coincides with the set P, but the partial order relation $\leq^\sharp$ on $P^\sharp$ satisfies the following condition:

$$\forall\, x, y \in P \qquad x \leq^\sharp y \text{ in } P^\sharp \Leftrightarrow y \leq x \text{ in } P.$$

Since we have that $x \leq^\sharp y$ is equivalent to writing $y \geq x$ in P, we can also denote the dual poset $P^\sharp$ by $(P, \geq)$.

Remark. Let $x \in P$ and, similarly as in (2.2), set

$$P_{\geq x} = \{s \in P \mid s \geq x\} \subseteq P.$$

Then $P_{\geq x}$ is a subposet of P and, according to [41], $P_{\geq x}$ is called a **dual order ideal** (or *up-set*) of P, which generally means an instance of a subset $D \subseteq P$ such that if $x \in D$ and $P \ni t \geq x$, then $t \in D$. Equivalently, $P_{\geq x}$ can be regarded as a principal order ideal of the dual poset $P^\sharp$. Again, we also have a subposet $P_{>x} = P_{\geq x} \setminus \{x\}$.

Let $(P, \leq_P)$ and $(Q, \leq_Q)$ be two posets. They are said to be **isomorphic** if there exists an *order-preserving bijection* $\varphi : P \to Q$ whose inverse is order-preserving, i.e.

$$x \leq_P y \quad \Leftrightarrow \quad \varphi(x) \leq_Q \varphi(y).$$

If a poset P and its dual $P^\sharp$ are isomorphic, then P is called **self-dual**.

If we have two or more posets, then there are also various operations that can be performed on them to get a new poset (see [41]). One of these operations is the direct product of posets, as defined below.

Definition 2.1.4. Let $(P, \leq_P)$ and $(Q, \leq_Q)$ be two posets. The **direct product** of P and Q is the poset $(P \times Q, \leq)$ which consists of the set $P \times Q = \{(x, y) \mid x \in P,\, y \in Q\}$ together with the partial order relation $\leq$ so that

$$(x, y) \leq (x', y') \text{ in } P \times Q \quad \Leftrightarrow \quad x \leq_P x' \text{ and } y \leq_Q y'\,.$$

Remark. Clearly, the map $(x, y) \mapsto (y, x)$, for all $x \in P$ and $y \in Q$, is an order-preserving bijection between the posets $P \times Q$ and $Q \times P$. Thus, $P \times Q$ and $Q \times P$ are isomorphic.

A poset P has a **minimum** $\hat{0}$ if there exists an element $\hat{0} \in P$ such that $\hat{0} \leq t$ for all $t \in P$. Similarly, P has a **maximum** $\hat{1}$ if there exists an element $\hat{1} \in P$ such that $t \leq \hat{1}$ for all $t \in P$. Both minimum and maximum are unique, if they exist.

Example 2.1.5.

(a) Assume that P is a poset with minimum $\hat{0}_P$ and Q is a poset with minimum $\hat{0}_Q$. Then $P \times Q$ has a minimum, i.e. $(\hat{0}_P, \hat{0}_Q)$. Similarly for the maximum, if P and Q have one.

(b) Let P be a poset with minimum $\hat{0}$. Then $P = P_{\geq \hat{0}}$. Moreover, if I is a non-empty order ideal of P, then $\hat{0} \in I$.

(c) Let $x \in P$ and consider $P_{\leq x}$ and $P_{\geq x}$ as subposets of $(P, \leq)$. Then x is the maximum of $P_{\leq x}$ and x in the minimum of $P_{\geq x}$.

Let $x, y \in P$ be two elements such that $x \leq y$. A closed **interval** (or *segment*) in P is the subset of all elements between x and y, ordered by $\leq$. Namely

$$[x, y] = \{z \in P \mid x \leq z \leq y\} = P_{\geq x} \cap P_{\leq y}.$$

P is called **locally finite** if every interval in P is finite.

If $s, t \in P$, then we say that s **is covered by** t if $s < t$ and $[s, t] = \{s, t\}$. So, we observe that a locally finite poset P is completely determined by its cover relations. The **Hasse diagram** of a finite poset P is the graph whose vertices are the elements of P, and whose edges are determined by the cover relations.

2.2 Lattices

Let $(P, \leq)$ be a poset and let S be a subset of P. We recall that $l \in P$ is a **lower bound** of S in P if $l \leq s$ for all $s \in S$. Let $W \subseteq P$ be the induced subposet whose elements are the lower bounds of S in P. If W has a maximum $\hat{1}_W$, then $\hat{1}_W$ is usually called the **greatest lower bound** of S in P. Similarly, we have that $u \in P$ is an **upper bound** of S in P if $s \leq u$ for all $s \in S$, and the **least upper bound** of S in P is the minimum (when it exists) of the induced subposet $U = \{u \in P \mid u \text{ is an upper bound of } S\} \subseteq P$.

Notation. Let $x, y \in P$. If $S = \{x, y\}$ and there exists the greatest lower bound l of S, then we denote l by $x \wedge y$ and we say that l is **the meet of** x **and** y in P. Similarly, if there exists the least upper bound u of S, then we denote u by $x \vee y$ and we say that u is **the join of** x **and** y in P.

A **lattice** is a poset $(L, \leq)$ such that for every pair of elements $x, y \in L$ there exist the meet $x \wedge y$ and the join $x \vee y$ in L. So, if L is a lattice, we can regard $\wedge$ and $\vee$ as two binary operations $L \times L \to L$. We observe that both

$\wedge$ and $\vee$ are associative, commutative and idempotent (i.e., $t \wedge t = t = t \vee t$). Let $Q \subseteq L$ be a subset such that Q is closed under these operations, i.e., if $x, y \in Q$ then $x \wedge y \in Q$ and $x \vee y \in Q$. Such a subset Q, endowed with the partial order relation $\leq$ induced by L, is a special case of a subposet of L which is called a **sublattice** of L.

Example 2.2.1.

(*a*) Every chain $(C, \leq)$ is a lattice. Indeed, x and y are comparable for every pair of elements $x, y \in C$. If $x \leq y$, then $x \wedge y = x$ and $x \vee y = y$. Obviously, every chain of a lattice L is a sublattice of L.

(*b*) If V is a vector space, let $\mathcal{S}_V$ denote the subspace lattice of V, i.e. the lattice whose elements are all the subspaces of V, ordered by inclusion. If $T, U \leq V$, then the meet of T and U in $\mathcal{S}_V$ is the intersection $T \cap U$, and their join is the sum $T + U = \{t + u \mid t \in T, u \in U\}$.

(*c*) If G is a group, let $\mathcal{L}(G)$ denote the subgroup lattice of G, i.e. the lattice whose elements are all the subgroups of G, ordered by inclusion. If $H, K \leq G$, then the meet of H and K in $\mathcal{L}(G)$ is the intersection $H \cap K$, and their join is the subgroup generated by H and K in G.

(*d*) The dual L^* of a lattice L is a lattice. If L_1 and L_2 are two lattices, then so is $L_1 \times L_2$.

(*e*) Let L be a lattice. Then, every closed interval $[x, y] \subseteq L$ is a sublattice.

For a lattice, the definition of an order ideal is exactly the same as the one given for a poset in Definition 2.1.2. So, for us, an order ideal of a lattice L is not necessarily a sublattice of L, since it might not be close under the operation of join $\vee$ (unlike what is required in [4]).

If $(L, \leq)$ is a finite lattice, such that $L = \{x_1, \ldots, x_n\}$, then clearly L has a maximum $\hat{1} = x_1 \vee \cdots \vee x_n$ and a minimum $\hat{0} = x_1 \wedge \cdots \wedge x_n$. Moreover, we introduce the following notion for finite lattices.

Definition 2.2.2. Let L be a finite lattice with minimum $\hat{0}$ and maximum $\hat{1}$. We say that L is **graded** if every maximal chain in L has the same length. In this case, we can recursively define a unique **rank function** $\mathrm{rk}_L : L \to \mathbb{N}$ such that

$$\begin{cases} \mathrm{rk}_L(\hat{0}) = 0\,; \\ \mathrm{rk}_L(y) = \mathrm{rk}_L(x) + 1 \quad \text{if } x \text{ is covered by } y. \end{cases}$$

Let C be a maximal chain of L, so that $\ell(C) = \ell(L) = n \in \mathbb{N}$. Then we have that $\mathrm{rk}_L(\hat{1}) = n$, and we say that the **rank of** L (i.e., its length) is n.

Remark. Finite graded posets are in fact defined in [41], and their definition can be extended to certain infinite posets. But we prefer to consider only finite lattices. Moreover, in the context of graded lattices, it is common to find the term *dimension* instead of *rank*, for instance in [4].

Example 2.2.3. Let $\mathcal{S}_V$ be the subspace lattice of a vector space V of dimension n over a finite field K. Clearly, each maximal chain of subspaces of V has length n, and therefore we have that $\mathcal{S}_V$ is graded of rank n. In particular, for each subspace $T \leq V$ the dimension $\dim_K(T)$ coincides with the value $\mathrm{rk}_{\mathcal{S}_V}(T)$ given by the rank function.

Let L be a finite lattice with minimum $\hat{0}$. An **atom** of L is an element $a \in L$ such that $\hat{0}$ is covered by a. The lattice L is said to be **atomistic** if every element of L is a join of atoms (we regard $\hat{0}$ as the join of the empty set of atoms). Dually, if L has a maximum $\hat{1}$, a **coatom** of L is an element which is covered by $\hat{1}$, and L is **coatomistic** if every element is a meet of coatoms. If L is finite and graded of rank n, then clearly $\mathrm{rk}_L(a) = 1$ for every atom of L, and $\mathrm{rk}_L(c) = n - 1$ for every coatom.

If x, y are elements of L such that $x \wedge y = \hat{0}$ and $x \vee y = \hat{1}$, then we say that x is a **complement** of y in L. A lattice L with minimum and maximum is **complemented** if every element of L has a complement.

Example 2.2.4. The subspace lattice $\mathcal{S}_V$ of a vector space $V \simeq K^n$ is both atomistic (and coatomistic) and complemented. On the contrary, if C is a finite chain of length $n \geq 2$, then C is neither atomistic nor complemented.

Now we recall a special type of elements which are particularly important for finite lattices, as we shall see.

Definition 2.2.5. Let L be a lattice. Let $x \in L$, so that $x \neq \hat{0}$ if L has a minimum $\hat{0}$. Then x is said to be **join-irreducible** if

$$x = y \vee z \quad \Rightarrow \quad \text{either } x = y \text{ or } x = z\,.$$

The subset of join-irreducible elements in L is denoted by $\mathrm{JI}(L)$

Dually, we can define the set $\mathrm{MI}(L)$ of **meet-irreducible** elements.

Remark. Let L be a finite lattice. Then we regard $\hat{0}$ as the join of the empty set of join-irreducible elements. Then every element of L can be written as the join of some join-irreducible elements in L (and, dually, also as the meet of some meet-irreducible elements of L). In particular, the atoms of L are join-irreducible (and the coatoms are meet-irreducible).

Example 2.2.6.

(*a*) Let $\mathcal{S}_V$ be the subspace lattice of a vector space $V \simeq K^n$. Since $\mathcal{S}_V$ is atomistic and the atoms of $\mathcal{S}_V$ are the 1-dimensional subspaces of V, we have that

$$\mathrm{JI}(\mathcal{S}_V) = \{T \leq V \mid \dim_K(T) = 1\}.$$

Dually, $\mathrm{MI}(\mathcal{S}_V) = \{T \leq V \mid \dim_K(T) = n - 1\}$ is the set of coatoms.

(*b*) Let C be a chain with minimum $\hat{0}_C$. Then every element $x \in C$, with $x \neq \hat{0}_C$, is join-irreducible in C.

(*c*) Let C_1 and C_2 be two chains, such that C_1 has minimum $\hat{0}_1$ and C_2 has minimum $\hat{0}_2$. Let $L = C_1 \times C_2$ be their direct product. Then every element $(x_1, x_2) \in L$ is the join of $(x_1, \hat{0}_2)$ and $(\hat{0}_1, x_2)$ in L. Thus,

$$\mathrm{JI}(L) = \{(x_1, \hat{0}_2), (\hat{0}_1, x_2) \mid \hat{0}_1 \neq x_1 \in C_1,\ \hat{0}_2 \neq x_2 \in C_2\}.$$

Now we focus on two special classes of lattices, which are particularly relevant from the combinatorial point of view. We shall connect them with the above notions and examples, with emphasis on finite lattices.

2.2.1 Modular and distributive lattices

Let $(L, \leq, \wedge, \vee)$ be a lattice. By using the definitions of $\wedge$ and $\vee$, it is almost immediate to see that the following inequality

$$u \vee (x \wedge y) \leq (u \vee x) \wedge (u \vee y) \tag{2.3}$$

holds for all $u, x, y, \in L$.

Now we fix $x, y \in L$, and consequently also the ordered pair $(x, y) \in L \times L$. We say that (x, y) is a **modular pair** if

$$\forall\, u \leq y \qquad u \vee (x \wedge y) = (u \vee x) \wedge y\,. \tag{2.4}$$

Definition 2.2.7. Let L be a lattice. Then L is **modular** if (x, y) is a modular pair for every $x, y \in L$.

Remark. Let L be a modular lattice. By inequality (2.3), to establish modularity of a pair (x, y) in L, it suffices to show that for all $u \in L$ we have

$$u \leq y \quad \Rightarrow \quad u \vee (x \wedge y) \geq (u \vee x) \wedge y\,. \tag{2.5}$$

We also observe that every sublattice of L is modular, since clearly modularity of the sublattice is induced by modularity of L.

Example 2.2.8.

(*a*) If x and y are comparable in L (i.e., $x \leq y$ or $y \leq x$), then it is easy to verify that the pair (x, y) is modular. Thus, every chain is a modular lattice.

(*b*) Let G be a group. Let $\mathcal{N}(G) = \{N \leq G \mid N \trianglelefteq G\}$ be the set of all normal subgroups of G. Then $\mathcal{N}(G)$ is a sublattice of the subgroup lattice $\mathcal{L}(G)$, where the join of two subgroups $H, K \in \mathcal{N}(G)$ is the subgroup HK. If $N \trianglelefteq G$ such that $N \leq K$, then it is not difficult to prove that

$$NH \cap K \leq (H \cap K)N\,.$$

Therefore, $\mathcal{N}(G)$ is modular.

(c) Let $\mathcal{S}_V$ be the subspace lattice of a vector space V. Then $\mathcal{S}_V$ is modular.

There are various ways to characterize modular lattices. An example is the so-called *Dedekind's modularity criterion*, which states that a lattice L is modular if and only if

$$\forall\, u, x, y \in L \qquad x \leq y,\ u \wedge x = u \wedge y,\ u \vee x = u \vee y \ \Rightarrow\ x = y.$$

For finite lattices, the following characterization is of particular interest and involves graded lattices.

Theorem 2.2.9. *Let L be a finite lattice. Then the three following conditions are equivalent.*

(i) *L is modular.*

(ii) *For all $x, y \in L$, we have that*

$$x \wedge y \text{ is covered by } x \quad \Leftrightarrow \quad y \text{ is covered by } x \vee y\,.$$

(iii) *L is graded, and its rank function rk_L satisfies*

$$\mathrm{rk}_L(x) + \mathrm{rk}_L(y) = \mathrm{rk}_L(x \wedge y) + \mathrm{rk}_L(x \vee y) \quad \forall\, x, y \in L\,.$$

The identity in (iii) corresponds to the well-known Grassmann Theorem for vector spaces, where the rank function on the subspace lattice $\mathcal{S}_V$ coincides with the dimension of subspaces.

Another important property of a finite modular lattice L concerns the different representations of an element in L as a join of some join-irreducible elements. Let $\bigvee_{i=1}^m x_i$ be the join of elements $x_1, \ldots, x_m \in L$. We recall that the join $\bigvee_{i=1}^m x_i$ is said to be **irredundant** if for every $k \in \{1, \ldots, m\}$

$$\bigvee_{i=1}^{m} x_i > x_1 \vee \cdots \vee x_{k-1} \vee x_{k+1} \vee \cdots \vee x_m = \bigvee_{j \neq k} x_j\,.$$

Theorem 2.2.10 (Kurosh-Ore)**.** *Let L be a finite modular lattice, and let $x \in L$, $x \neq \hat{0}$.*

(i) *If x has two representations $x = \bigvee_{i=1}^m y_i$ and $x = \bigvee_{j=1}^n z_j$ as joins of join-irreducible elements $y_1, \ldots, y_m, z_1, \ldots, z_n$ in L, then for every $i \in \{1, \ldots, m\}$ there exists $j \in \{1, \ldots, n\}$ such that*

$$x = y_1 \vee \cdots \vee y_{i-1} \vee z_j \vee y_{i+1} \vee \cdots \vee y_m\,.$$

(ii) *If x has two representations $x = \bigvee_{i=1}^m y_i$ and $x = \bigvee_{j=1}^n z_j$ as irredundant joins of elements $y_1, \ldots, y_m, z_1, \ldots, z_n \in \mathrm{JI}(L)$, then $m = n$.*

As a natural continuation of the Kurosh-Ore Theorem, we have Theorem 2.2.14 below. But we need firstly to recall the following important class of lattices.

Definition 2.2.11. A lattice L is **distributive** if

$$\forall\, u, x, y \in L \qquad u \vee (x \wedge y) = (u \vee x) \wedge (u \vee y)\,. \tag{2.6}$$

It is evident that distributivity condition (2.6) is a strengthening of modularity condition (2.4). By definition, in a distributive lattice L, every pair (x, y) of elements $x, y \in L$ is modular. So, if L is a distributive lattice, then L is modular.

Remark. Clearly, every sublattice of a distributive lattice is distributive.

We also observe that a lattice L is distributive if and only if

$$\forall\, u, x, y \in L \qquad u \wedge (x \vee y) = (u \wedge x) \vee (u \wedge y)\,. \tag{2.7}$$

Conditions (2.6) and (2.7) are the usual distributivity laws.

Example 2.2.12.

(a) Let X be a finite set, $|X| = n$. Then we denote by B_n the set of all subsets of X (so, $B_n = 2^X$), ordered by inclusion. With the operations of intersection $\cap$ and union $\cup$, the poset B_n is clearly a distributive lattice.

(b) Every chain is a distributive lattice. Moreover, if C_1 and C_2 are two chains, then $C_1 \times C_2$ is distributive too. The lattice B_n in (a) is isomorphic to the direct product of n chains of length 1.

(c) Let V be a vector space over a field K, such that $\dim_K(V) \geq 2$. We take two elements e_1, e_2 of the canonical basis of V. Let $\mathcal{S}_V$ be the subspace lattice of V. Let $T_1 = \langle e_1 \rangle$, $T_2 = \langle e_2 \rangle$, $T_3 = \langle e_1 + e_2 \rangle$ be elements of $\mathcal{S}_V$. Then it is immediate to see that

$$T_3 \cap (T_1 + T_2) \neq (T_3 \cap T_1) + (T_3 \cap T_2).$$

Thus, $\mathcal{S}_V$ is not distributive.

If L is a distributive lattice, the set (and subposet) $\mathrm{JI}(L)$ of join-irreducible elements in L has some nice features. Especially for finite distributive lattices, $\mathrm{JI}(L)$ reflects the structure of L. Here below, a property that we will use in section 4.4.

Proposition 2.2.13. *Let L be a distributive lattice and let $p \in \mathrm{JI}(L)$ be a join-irreducible element of L. If $p \leq x_1 \vee \cdots \vee x_n$ for some $x_1, \ldots, x_n \in L$, then $p \leq x_i$ for some $i \in \{1, \ldots, n\}$.*

Proof. By distributivity, we have

$$p = p \wedge (x_1 \vee \cdots \vee x_n) = (p \wedge x_1) \vee \cdots \vee (p \wedge x_n)\,.$$

Since $p \in \mathrm{JI}(L)$, then p must be equal to $p \wedge x_i$ for some i, whence $p \leq x_i$. □

If L is a finite distributive lattice and $x \in L$, we know that two different representations of x as a join of some join-irreducible elements have the same number of components, by Theorem 2.2.10. In fact, we have more: for a finite distributive lattice L, the representation of $x \in L$ as an irredundant join of some join-irreducible elements is unique, in the following sense.

Theorem 2.2.14. *Let L be a finite distributive lattice, and let $x \in L$, $x \neq \hat{0}$. If x has two representations $x = \bigvee_{i=1}^{m} y_i$ and $x = \bigvee_{j=1}^{n} z_j$ as irredundant joins of elements $y_1, \ldots, y_m, z_1, \ldots, z_n \in \mathrm{JI}(L)$, then $m = n$ and $\{y_1, \ldots, y_m\} = \{z_1, \ldots, z_m\}$.*

Corollary 2.2.15. *The rank of a finite distributive lattice is* $|\mathrm{JI}(L)|$.

Finally, there is a remarkable result that connects the structure of a finite distributive lattice L with the set of join irreducible elements in L. In particular, a role is played by the lattice of order ideals in the poset $\mathrm{JI}(L)$. But we need some notation.

Let P be a finite poset, so that $|P| = n$. Then we set

$$\mathcal{O}(P) = \{I \subseteq P \mid I \text{ is an order ideal of } P\}$$

the set of order ideals of P. Let I_1 and I_2 be two order ideals of P. Then both $I_1 \cap I_2$ and $I_1 \cup I_2$ are order ideals of P. So, we observe that $\mathcal{O}(P)$, ordered by inclusion, is isomorphic to a sublattice of B_n (as described in Example 2.2.12, (a)). In particular, $\mathcal{O}(P)$ is a distributive lattice.

Remark. An order ideal of P is a join-irreducible element in $\mathcal{O}(P)$ if and only if it is a principal ideal of P. Thus, since P is finite, we have that $I \in \mathrm{JI}(\mathcal{O}(P))$ if and only if $I = P_{\leq x}$ for some $x \in P$. Hence, there is a one-to-one correspondence between $\mathrm{JI}(\mathcal{O}(P))$ and P. Moreover, notice that $P_{\leq x} \subseteq P_{\leq y}$ if and only if $x \leq y$ in P. Hence,

$$\mathrm{JI}(\mathcal{O}(P)) \simeq P.$$

Since $\mathcal{O}(P)$ is a finite distributive lattice, we obtain that the rank of $\mathcal{O}(P)$ is $|P|$. By Theorem 2.2.14, for another poset Q, we have that $\mathcal{O}(P) \simeq \mathcal{O}(Q)$ if and only if $P \simeq Q$.

This information can be exploited to prove the following *Fundamental Theorem of Finite Distributive Lattices* (FTFDL).

Theorem 2.2.16 (FTFDL)**.** *Let L be a finite distributive lattice. Then there is an isomorphism*

$$L \simeq \mathcal{O}(\mathrm{JI}(L)) .$$

Moreover, if P is a poset such that $L \simeq \mathcal{O}(P)$, then $P \simeq \mathrm{JI}(L)$.

The isomorphism between L and $\mathcal{O}(\mathrm{JI}(L))$ is given by $f : L \to \mathcal{O}(\mathrm{JI}(L))$, so that

$$f(x) := \{a \in \mathrm{JI}(L) \mid a \leq x\} .$$

In the sense of Theorem 2.2.16, the structure of a finite distributive lattice is completely determined by its set of join-irreducible elements.

We recall that a lattice is said to be **boolean** if it is a complemented distributive lattice. The lattice B_n of Example 2.2.12 is a finite boolean lattice. By Theorem 2.2.16, every finite distributive lattice is isomorphic to a sublattice of a boolean lattice. We also observe that $|\mathrm{JI}(B_n)| = n$ and $\mathrm{JI}(B_n)$ is an antichain. As a consequence of Theorem 2.2.16, we have the following.

Corollary 2.2.17. *Let L be a finite distributive lattice. Then*

$$\begin{aligned} L \text{ is boolean} \quad &\Leftrightarrow \quad \mathrm{JI}(L) \text{ is an antichain;} \\ &\Leftrightarrow \quad \text{every } x \in \mathrm{JI}(L) \text{ is an atom of } L; \\ &\Leftrightarrow \quad \hat{1} \text{ is a join of atoms of } L; \\ &\Leftrightarrow \quad L \text{ is atomistic.} \end{aligned}$$

2.3 Subspace lattices induced by linear groups

In this section we consider in detail the subspace lattice $\mathcal{S}_V$ and some special sublattices $\mathcal{S}(V, H) \subseteq \mathcal{S}_V$ arising from the natural action of a group $H \leq \mathrm{GL}(V)$ on $\mathcal{S}_V$, induced by right matrix-vector multiplication. Although some general definitions can be given for any vector space V over a field K, we shall specify $V \simeq \mathbb{F}_q^n$ for some $n \in \mathbb{N}$ and q a prime power, if it is our interest that $\mathcal{S}(V, H)$ is finite.

Definition 2.3.1. Let V be a vector space over a field K. Let $h \in \mathrm{End}_K(V)$ be a K-linear endomorphism $h : V \to V$. We say that a subspace $W \leq V$ is **h-invariant** if $Wh \subseteq W$.

Notation. We denote by $\mathcal{S}(V, h)$ the set of all h-invariant subspaces of V:

$$\mathcal{S}(V, h) = \{W \leq V \mid W \text{ is } h\text{-invariant}\}.$$

We are mainly interested in the invertible endomorphisms $h : V \to V$, that is, the elements $h \in \mathrm{GL}(V)$, where $V \simeq K^n$ is a vector space of finite dimension over K. So, in this case, a subspace W of V is h-invariant if and only if $Wh = W$.

Remark. Let $h \in \mathrm{GL}(V)$ and let $A = \langle h \rangle$ be the subgroup of $\mathrm{GL}(V)$ generated by h. It is immediate to see that if $W \leq V$ is h-invariant, then W is h^k-invariant for all $h^k \in A$. Similarly, let $h_1, \ldots, h_r \in \mathrm{GL}(V)$ and consider the subgroup $B = \langle h_1, \ldots, h_r \rangle \leq \mathrm{GL}(V)$. Let $W \leq V$ be h_i-invariant for all $i = 1, \ldots, r$. Then W is b-invariant for all $b \in B$.

Definition 2.3.2. Let V be a vector space of finite dimension over K, and let $H \leq \mathrm{GL}(V)$. We say that a subspace $W \leq V$ is **H-invariant** if W is h-invariant for all $h \in H$.

Notation. We denote by $\mathcal{S}(V, H)$ the set of all H-invariant subspaces of V:

$$\mathcal{S}(V, H) = \bigcap_{h \in H} \mathcal{S}(V, h).$$

In particular, if $A = \langle h \rangle$ for some $h \in \mathrm{GL}(V)$, then $\mathcal{S}(V, A) = \mathcal{S}(V, h)$. And similarly, if $B = \langle h_1, \ldots, h_r \rangle \leq \mathrm{GL}(V)$, then $\mathcal{S}(V, B) = \bigcap_{i=1}^r \mathcal{S}(V, h_i)$.

Remark. Let $\mathcal{S}_V$ be the set of all subspaces of V, and let $G = \mathrm{GL}(\mathrm{V})$. There is an obvious action of G on $\mathcal{S}_V$ given by

$$\mathcal{S}_V \times G \ni (W, g) \mapsto W^g := Wg \in \mathcal{S}_V \,. \tag{2.8}$$

With respect to this action, we denote by $\mathrm{stab}_G(W)$ the set of all $g \in G$ such that $Wg = W$, i.e.

$$\mathrm{stab}_G(W) = \{g \in G \mid W \text{ is } g\text{-invariant}\}.$$

If H is a subgroup of $G = \mathrm{GL}(V)$, we have that

$$\mathcal{S}(V, H) = \{W \leq V \mid H \subseteq \mathrm{stab}_G(W)\}.$$

A subspace W of V is said to be **non-trivial** if $W \neq 0$ and $W \neq V$. Clearly, trivial subspaces 0 and V are element of $\mathcal{S}(V, H)$ for all $H \leq \mathrm{GL}(V)$.

Definition 2.3.3. Let H be a subgroup of $\mathrm{GL}(V)$. If there exists a non-trivial subgroup $W \leq V$ such that W is H-invariant, then H is called **reducible**. Otherwise, we say that H is **irreducible**.

In other terms, H is irreducible if and only if $\mathcal{S}(V, H) = \{0, V\}$.

Example 2.3.4.

(a) Let H be the trivial subgroup $1 \leq \mathrm{GL}(V)$. Then $\mathcal{S}(V, 1)$ is the set of all subspaces of V, i.e. $\mathcal{S}(V, 1) = \mathcal{S}_V$. Similarly, $\mathcal{S}(V, Z) = \mathcal{S}_V$, where $Z \leq \mathrm{GL}(V)$ is the centre of $\mathrm{GL}(V)$.

(*b*) Let $V = \bigoplus_{i=1}^{r} W_i$. We consider the subgroup $H \leq \mathrm{GL}(V)$ such that

$$H = \bigcap_{i=1}^{r} \mathrm{stab}_{\mathrm{GL}(V)} W_i \,,$$

where each stabilizer is defined with respect to the action of $\mathrm{GL}(V)$ on $\mathcal{S}_V$ as given in (2.8). Then, clearly, each $W_i \in \mathcal{S}(V,H)$. It is not difficult to see that a subspace $U \in \mathcal{S}(V,H)$ if and only if $U = \bigoplus_{j\in J} W_j$ for some $J \subseteq \{1,\dots,r\}$.

Indeed, for every $H \leq \mathrm{GL}(V)$, if $W_1, W_2 \in \mathcal{S}(V,H)$, then we have also $W_1+W_2 \in \mathcal{S}(V,H)$ and $W_1 \cap W_2 \in \mathcal{S}(V,H)$. It means that $\mathcal{S}(V,H)$ is closed under intersections and linear sums of subspaces, which are, respectively, the meet and join operations for the subspace lattice $\mathcal{S}_V$ ordered by inclusion. Thus, $(\mathcal{S}(V,H), \subseteq, \cap, +)$ is a modular lattice.

Proposition 2.3.5. *Let V be a vector space of finite dimension over K. Then $\mathcal{S}(V,H)$ is a sublattice of $\mathcal{S}_V$ for every subgroup $H \leq \mathrm{GL}(V)$. Hence $\mathcal{S}(V,H)$ is modular.*

As already observed above, 0 and V are elements in $\mathcal{S}(V,H)$ for every subgroup $H \leq \mathrm{GL}(V)$. Moreover, they are respectively the minimum and the maximum of $\mathcal{S}(V,H)$.

Remark. Let H and K be two subgroups of $\mathrm{GL}(V)$ such that $H \leq K$. Then $\mathcal{S}(V,K)$ is a sublattice of $\mathcal{S}(V,H)$.

Let $K = \mathbb{F}_q$ be the finite field with q elements. Then, for every subgroup $H \leq \mathrm{GL}(V)$ we have that $\mathcal{S}(V,H)$ is a finite lattice. Since $\mathcal{S}(V,H)$ is modular, by Theorem 2.2.9 it is also graded. Nevertheless, in this case the rank function defined on $\mathcal{S}(V,H)$ does not necessarily coincide with the dimension of subspaces.

Example 2.3.6. Let $K = \mathbb{F}_q$ and $V \simeq K^n$ such that $V = \bigoplus_{i=1}^{r} W_i$. Let H be as in (c) of Example 2.3.4. We have observed that there is a one-to-one correspondence between subspaces in $\mathcal{S}(V,H)$ and subsets of $\{1,\dots,r\}$. Let $U_1 = \bigoplus_{j\in J_1} W_j$ and $U_2 = \bigoplus_{j\in J_2} W_j$, with $J_1, J_2 \subseteq \{1,\dots,r\}$. Then $U_1 \leq U_2$ if and only if $J_1 \subseteq J_2$. Therefore $\mathcal{S}(V,H)$ is isomorphic to the boolean lattice B_r with r atoms. If there exists $i \in \{1,\dots,r\}$ such that $\dim_K(W_i) \geq 2$, then it is clear that there are subspaces $U \in \mathcal{S}(V,H)$ such that $\mathrm{rk}_{\mathcal{S}(V,H)}(U) \neq \dim_K(U)$.

Let $T \in \mathcal{S}(V,H)$ be an H-invariant subspace of V. The principal order ideal of $\mathcal{S}(V,H)$ generated by T is

$$\mathcal{S}(V,H)_{\leq T} = \{W \in \mathcal{S}(V,H) \mid W \leq T\}.$$

We immediately notice that $\mathcal{S}(V,H)_{\leq T}$ is also a sublattice of $\mathcal{S}(V,H)$. Then, 0 and T are respectively the minimum and maximum of $\mathcal{S}(V,H)_{\leq T}$, and $\mathcal{S}(V,H)_{\leq T}$ is modular.

Notation. We can also denote the ideal $\mathcal{S}(V,H)_{\leq T}$ by $\mathcal{S}(T,H)$, if the context allows it, i.e., if the vector space V is fixed and it is clear that H is a subgroup of $\mathrm{GL}(V)$.

Remark. Let $V \simeq \mathbb{F}_q^n$ and $H \leq \mathrm{GL}(V)$. Let $T \in \mathcal{S}(V,H)$. Then both $\mathcal{S}(V,H)$ and $\mathcal{S}(T,H)$ are graded lattices. We denote by rk_V and rk_T the rank functions defined on $\mathcal{S}(V,H)$ and $\mathcal{S}(T,H)$ respectively. Let $W \in \mathcal{S}(T,H)$. It is immediate to see that

$$\mathrm{rk}_V(W) = \mathrm{rk}_T(W).$$

So we can just write $\mathrm{rk}(W)$ to denote the rank of W in both of these lattices.

We know that every sublattice of a modular lattice is modular, and that every sublattice of a distributive lattice is distributive. But it is false, in general, that a sublattice of a boolean lattice is boolean. It is true, anyway, if we assume that $\mathcal{S}(V,H)$ is boolean and we consider the sublattice $\mathcal{S}(V,H)_{\leq T}$. Indeed, by Theorem 2.2.14 and Corollary 2.2.17, all the join-irreducible elements of $\mathcal{S}(V,H)_{\leq T}$ are the atoms of $\mathcal{S}(V,H)$ which are contained in T.

Proposition 2.3.7. *Let V be a vector space of finite dimension over $\mathbb{F}_q$. If $\mathcal{S}(V,H)$ is boolean, then $\mathcal{S}(V,H)_{\leq T}$ is boolean for every $T \in \mathcal{S}(V,H)$.*

Last thing we want to point out about H-invariant subspace lattice concerns quotient vector spaces. Let V be a vector space and $H \leq \mathrm{GL}(V)$. Let $W \in \mathcal{S}(V,H)$. Since W is H-invariant, there is a natural action of H on the quotient space V/W and its subspace lattice $\mathcal{S}_{V/W}$, such that for all $(W+X)/W \in \mathcal{S}_{V/W}$ and $h \in H$ we have

$$\left(\frac{W+X}{W}, h\right) \mapsto \left(\frac{W+X}{W}\right)^h := \frac{W+X^h}{W} = \frac{W+Xh}{W} \in \mathcal{S}_{V/W}\,. \tag{2.9}$$

For every subspace $X \leq V$, let $\overline{X} = (W+X)/W$. The set of H-invariant subspaces of V/W is therefore

$$\mathcal{S}(V/W,H) := \{\overline{X} \leq V/W \mid \overline{X}^h = \overline{X} \quad \forall\, h \in H\}.$$

In an obvious way, we can endow $\mathcal{S}(V/W,H)$ with the structure of a modular lattice.

2.3.1 Cyclic matrices

The structure of the H-invariant subspace lattice $\mathcal{S}(V,H)$ will play a significant role in issues addressed in the following chapters, where applications will concentrate on finite classical groups. In particular, Corollary 2.3.13 and Proposition 2.3.14 determine the structure of $\mathcal{S}(V,H)$ when H contains a cyclic matrix, by showing that in this case $\mathcal{S}(V,H)$ is a distributive lattice.

In §4.4 and §5.3 we will see in detail how this condition can be exploited for questions concerning the Möbius function of groups.

We remind our assumption that $V \simeq \mathbb{F}_q^n$ is a vector space of finite dimension over $\mathbb{F}_q$, and we identify $\mathrm{GL}(V)$ with the matrix group $\mathrm{GL}(n,q)$. Then we look for a “large” class of subgroups $H \leq \mathrm{GL}(V)$ so that $\mathcal{S}(V,H)$ has the nice property of being a finite distributive lattice.

For the sake of completeness, we could also recall here some elementary but useful notions of linear algebra. A general reference for this part is [18].

Let $\xi \in \mathrm{GL}(n,q)$.

- The **characteristic polynomial** of ξ is the polynomial $c_\xi(t) \in \mathbb{F}_q[t]$ such that $c_\xi(t) = \det(tI_n - \xi)$.
- The **minimal polynomial** of ξ is the unique monic polynomial of least degree $m_\xi(t) \in \mathbb{F}_q[t]$ such that $m_\xi(\xi) = 0$. It is the monic generator of

$$I_\xi = \{f(t) \in \mathbb{F}_q[t] \mid f(\xi) = 0\} \trianglelefteq \mathbb{F}_q[t]\,.$$

By Cayley-Hamilton Theorem, we know that $c_\xi(t) \in I_\xi$.

Definition 2.3.8. An element $\xi \in \mathrm{GL}(n,q)$ is said to be a **cyclic matrix** if its characteristic polynomial $c_\xi(t)$ equals its minimal polynomial $m_\xi(t)$.

Let $A \in \mathrm{GL}(V)$ and $w \in V$. The **A-module generated by** w is the span of $w, wA, wA^2, \ldots$ in V and it is denoted by $\langle w\rangle_A$. We have the following characterization for cyclic matrices, which explains their name.

Proposition 2.3.9. *Let $V \simeq \mathbb{F}_q^n$ and $\xi \in \mathrm{GL}(n,q)$. Then, ξ is a cyclic matrix if and only if there exists a vector $v \in V$ such that*

$$\langle v\rangle_\xi = \langle v, v\xi, \ldots, v\xi^{n-1}\rangle = V\,.$$

In this case, we refer to v as a **cyclic vector** for ξ on V, and we call (v,ξ) a **cyclic pair** for V.

Remark. Similarly, if a subspace $W \leq V$ is a ξ-module generated by a vector w, we call (w,ξ) a cyclic pair for W. We notice that $W = \langle w\rangle_\xi \in \mathcal{S}(V,\xi)$ and it is the smallest ξ-invariant subspace containing w.

Is it possible to determine a cyclic pair (w,ξ) for every $W \in \mathcal{S}(V,\xi)$? What information can we deduce about the structure of $\mathcal{S}(V,\xi)$? The following results provide a good answer to these questions for cyclic matrices.

Lemma 2.3.10. *Let $\xi \in \mathrm{GL}(n,q)$ be a cyclic matrix with minimal polynomial $m_\xi(t)$. Let v be a cyclic vector for ξ on $V \simeq \mathbb{F}_q^n$, such that $V = \langle v\rangle_\xi$. We assume that $m_\xi(t) = f_1(t)f_2(t)$ for some monic polynomials $f_1, f_2 \in \mathbb{F}_q[t]$. So, let $W = \langle vf_1(\xi)\rangle_\xi \leq V$ be the ξ-module generated by $vf_1(\xi)$, and denote by $\xi_{|W}$ the restriction of ξ to W. Then* (*i*) $f_2(t)$ *is the minimal polynomial of* $\xi_{|W}$*;*

(*ii*) $\dim(W) = \deg(f_2) = n - \deg(f_1)$*;*

(*iii*) $W = \ker(f_2(\xi))$.

As a consequence, we obtain that every $W \in \mathcal{S}(V, \xi)$ admits cyclic pair (w, ξ), for some $w \in V$, such that $\langle w \rangle_\xi = W$.

Proposition 2.3.11. *Let* $\xi \in \mathrm{GL}(n, q)$ *be a cyclic matrix with cyclic vector* $v \in V \simeq \mathbb{F}_q^n$*, such that* $V = \langle v \rangle_\xi$*. If* $W \in \mathcal{S}(V, \xi)$*, then*

(*i*) $W + v$ *is a cyclic vector for* ξ *on* V/W*.*

Let $\bar{c}(t) \in \mathbb{F}_q[t]$ *be the characteristic polynomial of* ξ *on* V/W*. Then*

(*ii*) $W = \langle v\bar{c}(\xi) \rangle_\xi$ *.*

Remark. In particular, we observe that if $\xi \in \mathrm{GL}(n, q)$ is a cyclic matrix and $W \leq V$ is an eigenspace of ξ, then $\dim(W) = 1$.

Now we put together the above information to describe $\mathcal{S}(V, \xi)$.

Theorem 2.3.12. *Let* $\xi \in \mathrm{GL}(n, q)$ *be a cyclic matrix with minimal polynomial* $m_\xi(t)$*, and denote by* $\mathcal{D}(m_\xi)$ *the set of all monic divisors of* $m_\xi(t)$ *in* $\mathbb{F}_q[t]$*. Let* v *be a cyclic vector for* ξ *on* $V \simeq \mathbb{F}_q^n$*, such that* $V = \langle v \rangle_\xi$*. Then*

$$\mathcal{S}(V, \xi) = \{\langle vf(\xi) \rangle_\xi \leq V \mid f(t) \in \mathcal{D}(m_\xi)\}.$$

In particular, if $m_\xi(t) = f(t)g(t)$, then $\langle vf(\xi) \rangle_\xi = \ker(g(\xi))$ by (*iii*) of Lemma 2.3.10. So, we also have that

$$\mathcal{S}(V, \xi) = \{\ker(g(\xi)) \leq V \mid g(t) \in \mathcal{D}(m_\xi)\}.$$

The set $\mathcal{D}(m_\xi)$, ordered by divisibility (i.e., $g_1(t) \leq g_2(t)$ if and only if $g_1(t) \mid g_2(t)$), turns out to be a lattice, where $g_1(t) \wedge g_2(t) = \gcd(g_1(t), g_2(t))$ is their monic greatest common divisor and $g_1(t) \vee g_2(t) = \mathrm{lcm}(g_1(t), g_2(t))$ is their monic lowest common multiple.

Corollary 2.3.13. *Let* $V \simeq \mathbb{F}_q^n$*. Let* $\xi \in \mathrm{GL}(n, q)$ *be a cyclic matrix with minimal polynomial* $m_\xi(t)$*, and denote by* $\mathcal{D}(m_\xi)$ *the lattice of all monic divisors of* $m_\xi(t)$ *in* $\mathbb{F}_q[t]$*. Then there is an isomorphism*

$$\mathcal{D}(m_\xi) \simeq \mathcal{S}(V, \xi)$$

given by the map $\mathcal{D}(m_\xi) \ni g(t) \mapsto \ker(g(\xi)) \leq V$*.*

Proof. The map $g(t) \mapsto \ker(g(\xi))$ is surjective by Theorem 2.3.12. Let $g_1(t), g_2(t) \in \mathbb{F}_q[t]$ be two monic divisors of $m_\xi(t)$. It is immediate to see that if $g_1(t)$ divides $g_2(t)$, then $\ker(g_1(\xi)) \subseteq \ker(g_2(\xi))$. And if $g_1(t) \neq g_2(t)$, then $\ker g_1(\eta) \neq \ker g_2(\eta)$. □

The structure of the lattice $\mathcal{D}(m_\xi)$ is well-known and depends on the prime factorization of $m_\xi(t)$ in $\mathbb{F}_q[t]$. Let

$$m_\xi(t) = f_1(t)^{\alpha_1} \cdot \ldots \cdot f_r(t)^{\alpha_r}$$

where $f_1(t), \ldots, f_r(t) \in \mathbb{F}_q[t]$ are monic and irreducible. Then

$$\mathcal{D}(m_\xi) \simeq \prod_{i=1}^{r} C(\alpha_i) = C(\alpha_1) \times \cdots \times C(\alpha_r)$$

where $\prod_{i=1}^{r} C(\alpha_i)$ denotes the direct product of r chains $C(\alpha_1), \ldots, C(\alpha_r)$ of length, respectively, $\alpha_1, \ldots, \alpha_r$. So, we have the following.

Proposition 2.3.14. *Let $V \simeq \mathbb{F}_q^n$ and let $\xi \in \mathrm{GL}(n,q)$ be a cyclic matrix. Then the lattice $\mathcal{S}(V,\xi)$ of ξ-invariant subspaces of V is isomorphic to a product of chains.*

Remark. In Example 2.2.12, we have seen that the direct product of chains is a distributive lattice. Therefore, if ξ is cyclic, $\mathcal{S}(V,\xi)$ is distributive. Moreover, for every subgroup $H \leq \mathrm{GL}(V)$ such that $\xi \in H$, we have that the lattice of H-invariant subspaces $\mathcal{S}(V,H)$ is distributive too, since every sublattice of a distributive lattice is distributive. From the point of view of abstract finite distributive lattices, a study on products of chains and the structure of their sublattices can be found in [39].

Since we are dealing with vector spaces, we can equivalently state Proposition 2.3.14 with the language of linear algebra, as Brickman and Fillmore do in [7].

Definition 2.3.15. Let V be a vector space and let $\mathcal{L}$ be a sublattice of the subspace lattice $\mathcal{S}_V$. Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be two sublattices of $\mathcal{L}$. Then $\mathcal{L}$ is the **direct sum** of $\mathcal{L}_1$ and $\mathcal{L}_2$ if $W_1 \cap W_2 = 0$ for all $W_1 \in \mathcal{L}_1$, $W_2 \in \mathcal{L}_2$, and

$$\mathcal{L} = \{W_1 \oplus W_2 \mid W_1 \in \mathcal{L}_1,\ W_2 \in \mathcal{L}_2\}.$$

The lattice operations can be performed *coordinate-wise* and clearly, in this case, $\mathcal{L} \simeq \mathcal{L}_1 \times \mathcal{L}_2$.

A lattice of subspaces of V that cannot be written as a non-trivial direct sum is called **$\oplus$-irreducible**.

By Corollary 2.3.13, we have that Proposition 2.3.14 is equivalent to saying that the lattice $\mathcal{S}(V,\xi)$ is a direct sum of sublattices $\mathcal{L}_1, \ldots, \mathcal{L}_r$ so that every $\mathcal{L}_i$ is a chain of ξ-invariant subspaces with minimum 0 and maximum V_i. Then every $W \in \mathcal{S}(V,\xi)$ is uniquely representable in the form $W = W_1 \oplus \cdots \oplus W_r$, where each $W_i \in \mathcal{L}_i$. In particular, $0 = 0 \oplus \cdots \oplus 0$ and $V = V_1 \oplus \cdots \oplus V_r$. We also notice that every chain $\mathcal{L}_i$ is $\oplus$-irreducible.

Remark. It is interesting to note that, even if ξ is not a cyclic matrix, $\mathcal{S}(V,\xi)$ has the structure of a direct sum of $\oplus$-irreducible sublattices. In this case, nevertheless, there exists $i \in \{1,\dots,r\}$ such that L_i is not a chain, and $\mathcal{S}(V,\xi)$ is not distributive (see [7, Theorem 2] for details).

At this point, can we say something about the number of subgroups $H \leq \mathrm{GL}(n,q)$ with the property that $\mathcal{S}(V,H)$ is a distributive lattice? Maybe we do not have a precise answer, but we can think that from a cyclic matrix $\xi \in \mathrm{GL}(n,q)$ we can move to the subgroup $\langle\xi\rangle$ generated by ξ, and, more generally, to all subgroups $H \leq \mathrm{GL}(n,q)$ containing ξ. For such subgroups, we even know that $\mathcal{S}(V,H)$ is a sublattice of a product of chains. So, first of all, we are interested in estimates on the number of cyclic matrices in $\mathrm{GL}(n,q)$.

Remark. All conjugates of a matrix $\xi \in \mathrm{GL}(n,q)$ have the same characteristic polynomial and the same minimal polynomial. So, if ξ is a cyclic matrix, then all conjugates of ξ in $\mathrm{GL}(n,q)$ are cyclic matrices.

Conversely, are two cyclic matrices similar, if they have the same minimal polynomial?

Example 2.3.16. Let $\xi \in \mathrm{GL}(n,q)$ be an irreducible matrix, which means that $\mathcal{S}(V,\xi) = \{0,V\}$. Let $v \in V$, $v \neq 0$. Then we have that $\langle v\rangle_\xi = V$ and, by Proposition 2.3.9, the matrix ξ is cyclic. Since the vectors $v, v\xi, \dots, v\xi^{n-1}$ form a basis of V, the matrix ξ is similar to

$$\varXi_{m_\xi} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{n-1} \end{pmatrix} \tag{2.10}$$

such that $v\xi^n = -c_0 v - c_1 v\xi - \ldots - c_{n-1} v\xi^{n-1}$. Then

$$m_\xi(t) = t^n + c_{n-1}t^{n-1} + \ldots + c_1 t + c_0$$

is the minimal polynomial of ξ in $\mathbb{F}_q[t]$. It follows that every irreducible matrix in $\mathrm{GL}(n,q)$ with minimal polynomial $m_\xi(t)$ is similar to $\varXi_{m_\xi}$. Hence all irreducible matrices with the same characteristic polynomial are similar.

This can be generalized for all cyclic matrices in $\mathrm{GL}(n,q)$.

Proposition 2.3.17. *Let $\xi \in \mathrm{GL}(n,q)$ be a cyclic matrix with minimal polynomial $m_\xi(t)$. Then ξ is similar to a matrix $\varXi_{m_\xi}$ as in* (2.10)*, such that $m_\xi(t) = t^n + c_{n-1}t^{n-1} + \ldots + c_1 t + c_0$. Moreover, ξ is conjugate to any other cyclic matrix in* $\mathrm{GL}(n,q)$ *with the same minimal polynomial.*

Now, let $f(t) \in \mathbb{F}_q[t]$ be a monic polynomial

$$f(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0$$

such that $f(0) = a_0 \neq 0$. Then, we have the **companion matrix** of $f(t)$ in $\mathrm{GL}(n, q)$, that is

$$\varXi_f = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{pmatrix}.$$

Clearly, $\varXi_f$ is a cyclic matrix with minimal polynomial $f(t)$.

Thanks to estimates on the number of monic irreducible polynomials of degree r over $\mathbb{F}_q$, and by using the correspondence between minimal polynomials and companion matrices, Praeger and Neumann make precise the assertion that almost all matrices in $\mathrm{GL}(n, q)$ are cyclic, in the following sense (see [30] and [31]).

Theorem 2.3.18. *Let* $\mathrm{Cyc}(n, q)$ *be the set of all cyclic matrices in* $\mathrm{GL}(n, q)$. *Let*

$$P(\mathrm{Cyc}(n, q)) = \frac{|\mathrm{Cyc}(n, q)|}{|\mathrm{GL}(n, q)|}$$

be the probability that a matrix in $\mathrm{GL}(n, q)$ *is cyclic. Then, for all* $n \geq 1$ *and prime powers* q

$$1 - P(\mathrm{Cyc}(n, q)) \leq \frac{1}{q(q^2 - 1)}.$$

In particular, if $n = 1$, then $\mathrm{Cyc}(1, q) = \mathrm{GL}(1, q)$ and $P(\mathrm{Cyc}(1, q)) = 1$. If $n = 2$, then a matrix $\xi \in \mathrm{GL}(2, q)$ is non-cyclic if and only if ξ is scalar, i.e. ξ is in the centre of $\mathrm{GL}(n, q)$. Since $|\mathrm{GL}(2, q)| = q(q^2 - 1)(q - 1)$ and $|Z(\mathrm{GL}(2, q))| = q - 1$, we have that

$$1 - P(\mathrm{Cyc}(2, q)) = 1/q(q^2 - 1).$$

If $n \geq 3$, then Praeger and Neumann show that

$$1 - P(\mathrm{Cyc}(n, q)) < 1/q(q^2 - 1).$$

In fact, in [30], they achieve upper and lower bounds for $P(\mathrm{Cyc}(n, q))$, which are enough to establish that $P(\mathrm{Cyc}(n, q)) = 1 - q^{-3} + O(q^{-4})$. Actually, the proportion of cyclic matrices in any group containing $\mathrm{SL}(n, q)$ is not much different from this, and in [31] they obtain similar estimations for other irreducible finite classical groups. Moreover, if we fix q and look at the limit, as $n \to \infty$, of the probability that an element of $\mathrm{GL}(n,q)$ is cyclic, we obtain

$$P(\mathrm{Cyc}(n,q)) \to \frac{1-q^{-5}}{1-q^{-3}}$$

(see [43, Equation 6.24]). Finally, in his PhD thesis [8], Brown extends such results to maximal reducible subgroups of $\mathrm{GL}(n,q)$.

Since most of the elements in $\mathrm{GL}(n,q)$ are cyclic matrices, it seems reasonable to choose and study $\mathcal{S}(V,H)$ when the subgroup $H \leq \mathrm{GL}(n,q)$ contains a cyclic matrix, in the sense that such subgroups constitute a remarkably large class of subgroups of $\mathrm{GL}(n,q)$. This motivates the choice of focussing on distributive lattices $\mathcal{S}(V,H)$ in Chapter 4 and Chapter 5, where we will deal with problems concerning the subgroup lattice of $\mathrm{GL}(n,q)$.

Remark. Instead of the probability of finding a cyclic matrix in $\mathrm{GL}(n,q)$, it may also be interesting to study the following question.

Question. *What is the proportion of subgroups which contain some cyclic matrix among all subgroups of* $\mathrm{GL}(n,q)$*?*

Chapter 3

The Möbius function

The Möbius function of locally finite partially ordered sets is a classical tool in enumerative combinatorics, and it generalizes the number-theoretic Möbius function $\mu : \mathbb{N} \to \mathbb{Z}$ defined, for any positive integer n, as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^r & \text{if } n = p_1 \cdot \ldots \cdot p_r \,, \text{ with prime factors } \; p_i \neq p_j \; \forall i \neq j \\ 0 & \text{if } n \text{ is divisible by } p^2 \,, \text{ for some } p \text{ prime.} \end{cases}$$

We want to introduce such a generalization and state the related key results that will be used in the following chapters, where we will develop some methods in order to compute the Möbius function for finite classical groups. This chapter is therefore divided into two main sections. In §3.1 we collect some facts concerning the Möbius function of abstract locally finite posets ([41] is the main reference for this part). In section §3.2, we try to motivate our interest in connections between the Möbius function and the theory of groups through stimulating open questions. Some basic knowledge is assumed both for finite and profinite groups. We refer to [35] and [44] for the necessary general background.

3.1 The Möbius function of locally finite posets

Let $(P, \leq)$ be a poset. We assume that every interval

$$[x, y] = \{t \in P \mid x \leq t \leq y\}$$

in P is finite, so that P is locally finite.

Definition 3.1.1. The **Möbius function** associated with a locally finite poset P is a map $\mu_P : P \times P \to \mathbb{Z}$ satisfying

$$\mu_P(x, y) = 0 \quad \text{unless } \; x \leq y \,,$$

and defined recursively for $x \leq y$ by

$$\mu_P(x,x) = 1 \qquad \text{and} \qquad \sum_{x \leq t \leq y} \mu_P(x,t) = 0 \;\text{ if }\; x < y\,. \tag{3.1}$$

Notation. Let S be an interval $[x,y]$ of P. It is clear, by definition, that the Möbius function μ_S of S equals the restriction of μ_P to S. So, we can simply use μ to denote both μ_P and its restriction μ_S, if the context allows it.

Example 3.1.2.

(a) Let C be a finite chain and $x,y \in C$. Then

$$\mu(x,y) = \begin{cases} 1 & \text{if } x = y\,; \\ -1 & \text{if } x \text{ is covered by } y\,; \\ 0 & \text{otherwise.} \end{cases}$$

(b) Let P and Q be two locally finite posets, and let $P \times Q$ be their direct product. If $(x_1,y_1) \leq (x_2,y_2)$ in $P \times Q$, then the interval $[(x_1,y_1),(x_2,y_2)]$ is finite and

$$\mu_{P\times Q}((x_1,y_1),(x_2,y_2)) = \mu_P(x_1,x_2) \cdot \mu_Q(y_1,y_2)\,.$$

Indeed, if $(x_1,y_1) = (x_2,y_2)$, then $\mu_P(x_1,x_2) \cdot \mu_Q(y_1,y_2) = 1$. Otherwise, if $(x_1,y_1) < (x_2,y_2)$, then it is immediate to see that

$$\sum_{(x_1,y_1) \leq (t,u) \leq (x_2,y_2)} \mu_P(x_1,t) \cdot \mu_Q(y_1,u) = 0\,.$$

Hence (3.1) is satisfied and it determines $\mu_{P\times Q}((x_1,y_1),(x_2,y_2))$ uniquely.

(c) Let $r \in \mathbb{N}$. By combining (a) and (b) above, we can determine the Möbius function of a direct product P of r locally finite chains. W.l.o.g., we can assume that each chain has finite length ≥ 1 and we can compute $\mu_P(\hat{0},\hat{1})$, where $\hat{0}$ and $\hat{1}$ are the minimum and maximum of P, respectively. If all chains have length 1, then P is isomorphic to the boolean lattice B_r and $\mu_P(\hat{0},\hat{1}) = (-1)^r$. Otherwise, if there exists a chain of length ≥ 2, then $\mu_P(\hat{0},\hat{1}) = 0$. We will extend this example with Theorem 3.1.14 in §3.1.1.

(d) By applying (c), it is immediate now to represent the number-theoretic Möbius function $\mu : \mathbb{N} \to \{0, \pm 1\}$ through the Möbius function of a locally finite poset. Let $P = (\mathbb{N}, \preceq)$, so that $m \preceq n \Leftrightarrow m|n$. P is a locally finite poset and the interval $[1,n]$ in P is isomorphic to a direct product of chains. Thus,

$$\mu_P(1,n) = \mu\,(n) \qquad \forall\, n \in \mathbb{N}\,.$$

(*e*) Let $V \simeq \mathbb{F}_q^n$ and let $\mathcal{S}_V$ be the subspace lattice of V. If $U \leq W$ in $\mathcal{S}_V$, then the interval $[U, W]$ is isomorphic to the subspace lattice of $W/U \simeq \mathbb{F}_q^m$ for some $m \leq n$. Therefore, $\mu(U, W)$ in $\mathcal{S}_V$ depends only on the dimension of the quotient space W/U. We will show how to easily compute $\mu(0, V)$, by using Theorem 3.1.10.

Let x and y be two elements of the poset P, such that $x \leq y$. Let $C \subseteq P$ be a chain such that its minimum is x and its maximum is y. Then, we say that C is a **chain from** x **to** y. In a finite interval $[x, y]$, the chains from x to y determine the Möbius function of the interval, as follows.

Theorem 3.1.3 (P. Hall)**.** *Let $(P, \leq)$ be a locally finite poset, and let $x, y \in P$ such that $x \leq y$. Then*

$$\mu(x, y) = \sum_{C \in \mathcal{K}_{x,y}} (-1)^{\ell(C)}$$

where $\mathcal{K}_{x,y} = \{C \subseteq P \mid C \text{ is a chain from } x \text{ to } y\}$.

Hall's Theorem can be easily proven by induction on the length of $[x, y]$ and it provides a tool which is useful to characterize and estimate the Möbius function on several occasions.

Example 3.1.4. Let P be a locally finite poset and $P^\sharp$ its dual. If $[x, y]$ is an interval in P, then

$$[y, x] = \{t \in P^\sharp \mid y \geq t \geq x\} \subseteq P^\sharp$$

is a finite interval in $P^\sharp$, and it is essentially the dual of $[x, y]$. Let $\mathcal{K}_{x,y}$ be the set of all chains from x to y in P, and let $\mathcal{K}^\sharp_{y,x}$ be the set of all chains from y to x in $P^\sharp$. Clearly, there is a one-to-one correspondence from $\mathcal{K}_{x,y}$ to $\mathcal{K}^\sharp_{y,x}$, such that every chain of length r in $\mathcal{K}_{x,y}$ corresponds to a chain of length r in $\mathcal{K}^\sharp_{y,x}$. Therefore, by Proposition 3.1.3 we have that

$$\mu(x, y) = \mu^\sharp(y, x)\,, \tag{3.2}$$

where μ is the Möbius function of P and $\mu^\sharp$ is the Möbius function of $P^\sharp$.

Remark. If we apply the recursive formula of Definition 3.1.1 to the Möbius function $\mu^\sharp$ of the dual poset $P^\sharp$, for $y > x$ in $P^\sharp$ we have that (3.1) turns into

$$\sum_{y \geq t \geq x} \mu^\sharp(y, t) = 0\,,$$

which can be equivalently written as

$$\sum_{x \leq t \leq y} \mu(t, y) = 0\,.$$

by (3.2) of Example 3.1.4. So, for $x \leq y$ in P, the Möbius function of P can be defined also by

$$\mu(y,y) = 1 \qquad \text{and} \qquad \sum_{x \leq t \leq y} \mu(t,y) = 0 \ \text{ if } \ x < y\,. \tag{3.3}$$

Depending on the specific circumstances, sometimes (3.3) is more convenient than considering (3.1).

If L is a locally finite lattice, then each interval $[x,y]$ in L is a finite lattice. So, we may assume that L is a finite lattice with minimum $\hat{0}$ and maximum $\hat{1}$. We are interested in $\mu_L(\hat{0},x)$ and $\mu_L(x,\hat{1})$ for $x \in L$. The following result is often helpful, because it allows us to ignore all elements which are not meets of coatoms or, dually, which are not joins of atoms.

Proposition 3.1.5. *Let L be a finite lattice. Let M be the set of coatoms in L, and N be the set of atoms in L.*

(*i*) *Let $M^\wedge = \{x_1 \wedge \cdots \wedge x_r \in L \mid x_1, \ldots, x_r \in M,\ r \geq 1\} \cup \{\hat{1}\}$. Then*

$$\begin{cases} \mu_L(x,\hat{1}) = \mu_{M^\wedge}(x,\hat{1}) & \text{if } x \in M^\wedge \\ \mu_L(x,\hat{1}) = 0 & \text{otherwise.} \end{cases}$$

(*ii*) *Let $N^\vee = \{y_1 \vee \cdots \vee y_r \in L \mid y_1, \ldots, y_r \in N,\ r \geq 1\} \cup \{\hat{0}\}$. Then*

$$\begin{cases} \mu_L(\hat{0},y) = \mu_{N^\vee}(\hat{0},y) & \text{if } x \in N^\vee \\ \mu_L(\hat{0},y) = 0 & \text{otherwise.} \end{cases}$$

Both (*i*) and (*ii*) in Proposition 3.1.5 can be easily proven by induction on the length of $[x,\hat{1}]$ and $[\hat{0},y]$, respectively. We want to observe that this kind of proof needs Definition 3.1.1 for (*ii*) and the equivalent definition as in (3.3) above for (*i*). Proposition 3.1.5 can also be considered as a corollary of the next more general result, which is referred to as the *Crosscut Theorem.*

Theorem 3.1.6 (Crosscut Theorem). *Let L be a finite lattice with minimum $\hat{0}$ and maximum $\hat{1}$, so that $\hat{0} \neq \hat{1}$. Let M be the set of all coatoms in L. Let $X \subseteq L$ be a subset such that $M \subseteq X$ and $\hat{1} \notin X$. Then*

$$\mu_L(\hat{0},\hat{1}) = \sum_{Y \in \mathcal{Y}} (-1)^{|Y|}$$

where

$$\mathcal{Y} = \{Y \subseteq X \ \mid Y \neq \emptyset \ \text{ and } \ \bigwedge_{y \in Y} y = \hat{0}\,\}\,.$$

Consequently, assuming $X = M$, we can say that $\mu_L(\hat{0}, \hat{1})$ is the difference between the number of ways to express $\hat{0}$ as a meet of evenly many coatoms in L and the number of ways to express it as a meet of oddly many coatoms. In particular, if $\hat{0}$ is not a meet of coatoms in L, then $\mu_L(\hat{0}, \hat{1}) = 0$.

Remark. In the dual version of the Crosscut Theorem, N is the set of all atoms and it takes the place of M above. Then we assume that $X \subseteq L$ is a subset so that $N \subseteq X$ and $\hat{0} \notin X$. The conclusion is essentially the same, but we have to use the joins of elements in X that are equal to $\hat{1}$.

Among other applications, Theorem 3.1.3 and Theorem 3.1.6 establish an interesting connection between combinatorics and algebraic topology. The bridge between these two areas is an interpretation of the Möbius function as a reduced Euler characteristic of a special simplicial complex (for elementary definitions, see for instance [29]). We mention the main result, giving a brief description, but we refer to [41] for all details.

Let P be a finite poset and let $\widehat{P}$ denote $\{\hat{0}\} \cup P \cup \{\hat{1}\}$, i.e. P with an extra minimum $\hat{0}$ and an extra maximum $\hat{1}$ adjoined. Then, by Theorem 3.1.3, we have that

$$\mu_{\widehat{P}}(\hat{0}, \hat{1}) = -\gamma_1 + \gamma_2 - \gamma_3 + \dots \tag{3.4}$$

where each γ_i is the number of chains of length i from $\hat{0}$ to $\hat{1}$ in $\widehat{P}$. Clearly, if we consider a chain $\hat{0} = x_0 < x_1 < \dots < x_{i-1} < x_i = \hat{1}$ of length i in $\widehat{P}$, then $x_1 < \dots < x_{i-1}$ is a chain of length $i-2$ in P. We observe that $\gamma_1 = 1$.

Now, for the same finite poset P, we define the simplicial complex $\sigma(P)$ as follows. The vertices of $\sigma(P)$ are the elements of P, and the faces of $\sigma(P)$ are the chains of P. This is the reason why $\sigma(P)$ is called the **order complex** of P. We remind that the **Euler characteristic** of $\sigma(P)$ is

$$\chi(\sigma(P)) = \sum_i (-1)^i F_i = F_0 - F_1 + F_2 - F_3 + \dots \tag{3.5}$$

where each F_i is the number of i-faces of $\sigma(P)$. Topologically, a 0-face is a single point (i.e., a chain of length 0 in P), a 1-face is a segment (i.e., a chain of length 1 in P), etc., so that we have that $F_i = \gamma_{i+2}$ for all $i \geq 0$.

Proposition 3.1.7. *Let P be a finite poset. Then*

$$\mu_{\widehat{P}}(\hat{0}, \hat{1}) = \widetilde{\chi}(\sigma(P)) \tag{3.6}$$

where $\widetilde{\chi}(\sigma(P)) = \chi(\sigma(P)) - 1$.

$\widetilde{\chi}(\sigma(P))$ is the so-called **reduced Euler characteristic** of $\sigma(P)$, which also counts $-F_{-1} = -1$ in (3.5), where F_{-1} is the number of -1-faces of $\sigma(P)$. There exists a unique -1-face, that is the empty face $\emptyset$ of $\sigma(P)$.

Remark. If L is a finite lattice, there exist a minimum $\hat{0}$ and a maximum $\hat{1}$ in L (and we may always assume $\hat{0} \neq \hat{1}$). Let $L^* = L \setminus \{\hat{0}, \hat{1}\}$ be the subposet of L given by L without minimum and maximum. Then (3.6) turns into

$$\mu_L(\hat{0}, \hat{1}) = \widetilde{\chi}(\sigma(L^*)). \tag{3.7}$$

Moreover, let X and $\mathcal{Y}$ be the same set as in Theorem 3.1.6, so that

$$\mu_L(\hat{0}, \hat{1}) = \sum_{Y \in \mathcal{Y}} (-1)^{|Y|},$$

and define $\mathcal{Y}^{\complement} := \{Y \subseteq X \mid \bigwedge_{y \in Y} y \neq \hat{0}\} \cup \{\emptyset\}$. Thus, we have that

$$\mu_L(\hat{0}, \hat{1}) = -\sum_{Y \in \mathcal{Y}^{\complement}} (-1)^{|Y|} = \sum_{Y \in \mathcal{Y}^{\complement}} (-1)^{|Y|-1}$$

and, if we identify $\mathcal{Y}^{\complement}$ with a simplicial complex, we obtain

$$\widetilde{\chi}(\sigma(L^*)) = \mu_L(\hat{0}, \hat{1}) = \widetilde{\chi}(\mathcal{Y}^{\complement}). \tag{3.8}$$

This proximity of the Möbius function to topological objects can be noticed also in the following theorem, known as *Crapo's Closure Theorem.*

Definition 3.1.8. Given a partially ordered set $(P, \leq)$, a **closure operator** on P is a function $c : P \to P$ satisfying the following three conditions:

- $\forall x \in P \quad x \leq c(x)$;
- $\forall x, y \in P \quad x \leq y \Rightarrow c(x) \leq c(y)$;
- $\forall x \in P \quad c(c(x)) = c(x)$.

Notation. The closure can be denoted by $\bar{\ }: P \to P$ and $x \mapsto \bar{x}$.

By analogy to topology, an element x in P is said to be **closed** with respect to the closure c if $c(x) = x$. Then

$$\overline{P} = \{x \in \mathcal{X} \mid c(x) = x\}$$

is the subposet of closed elements in P.

If P is locally finite and c is a closure operator on P, then $\overline{P}$ is locally finite. Let μ_P and $\mu_{\overline{P}}$ be the Möbius functions of P and $\overline{P}$, respectively.

Theorem 3.1.9 (Crapo's closure theorem)**.** *Let P be a locally finite poset and let $c : P \to P$ be a closure operator on P. Fix $x, y \in P$ so that $c(y) = y \in \overline{P}$. Then*

$$\sum_{z \in Y} \mu_P(x, z) = \begin{cases} \mu_{\overline{P}}(x, y) & \textit{if } x = c(x) \\ 0 & \textit{otherwise} \end{cases}$$

where $Y = \{z \in P \mid c(z) = y\}$.

A proof can be found in [12]. Moreover, in [11] there is another remarkable theorem due to Crapo that we want to mention.

Theorem 3.1.10 (Crapo's complement theorem). *Let L be a finite lattice with minimum $\hat{0}$ and maximum $\hat{1}$. Let $x \in L$ and let $x^{\perp}$ be the set of complements to x in L. Then*

$$\mu(\hat{0}, \hat{1}) = \sum_{y,z \in x^{\perp}} \mu(\hat{0}, y)\zeta(y, z)\mu(z, \hat{1})$$

where $\zeta : P \times P \to \mathbb{Z}$ is defined as

$$\zeta(y, z) = \begin{cases} 1 & \text{if } y \leq z\,; \\ 0 & \text{otherwise.} \end{cases}$$

In particular, if $x^{\perp}$ is an antichain, then we have

$$\mu(\hat{0}, \hat{1}) = \sum_{y \in x^{\perp}} \mu(\hat{0}, y)\mu(y, \hat{1})\,. \tag{3.9}$$

As an immediate application, we can use (3.9) to compute $\mu(0, V_n)$ on the subspace lattice $\mathcal{S}_{V_n}$ of a vector space $V_n \simeq \mathbb{F}_q^n$, in the following way. Let $T \in \mathcal{S}_{V_n}$ be a subspace of V of dimension 1. We notice that a complement of T in $\mathcal{S}_{V_n}$ is a subspace W of dimension $n-1$ such that $T \not\leq W$. We observe that such a complement W is a coatom of $\mathcal{S}_{V_n}$, hence $\mu(W, V) = -1$. Moreover, for each complement W we have that $\mu(0, W) = \mu(0, V_{n-1})$, where $V_{n-1} \simeq \mathbb{F}_q^{n-1}$. By (3.9), we obtain that

$$\mu(0, V_n) = -\sum_{W \in T^{\perp}} \mu(0, V_{n-1}) = -|T^{\perp}| \cdot \mu(0, V_{n-1})$$

where $T^{\perp}$ is the set of complements of T. So, we need the number of complements of T. The number of subspaces of V_n dimension $n-1$ is

$$\binom{n}{n-1}_q = q^{n-1} + q^{n-2} + \cdots + 1\,,$$

and the number of subspaces of dimension $n-1$ containing T is equal to the number of subspace of dimension $n-2$ in $V_n/T \simeq V_{n-1}$, that is

$$\binom{n-1}{n-2}_q = q^{n-2} + q^{n-3} + \cdots + 1\,.$$

We conclude that $\mu(0, V_n) = -q^{n-1}\mu(0, V_{n-1})$. By induction, there follows that

$$\mu(0, V_n) = (-1)^n q^{n-1} q^{n-2} \ldots q = (-1)^n q^{\binom{n}{2}}\,. \tag{3.10}$$

3.1.1 Order ideals and finite distributive lattices

Now we want to highlight some results which directly involve order ideals. In the following chapters, it will become clearer why we look at the role of these structures with special interest. The following is a natural generalization of the number-theoretic *Möbius inversion formula.*

Theorem 3.1.11 (Möbius inversion formula). *Let P be poset for which every principal order ideal is finite. Let K be a field and $f : P \to K$ be a function. For all $x \in P$, let*

$$g(x) = \sum_{y \leq x} f(y).$$

Then, for all $x \in P$ we have that

$$f(x) = \sum_{y \leq x} g(y)\mu(y, x)$$

where μ is the Möbius function of the principal order ideal $P_{\leq x}$.

Example 3.1.12. Theorem 3.1.11, combined with equation (3.10), can be used to count the number of spanning subsets of a vector space $V \simeq \mathbb{F}_q^n$. This result can be found in [41] and the same idea can be actually applied to determine the number of generating sets for a finite group. We will focus on such a question in §3.2.

Let L be a finite lattice with minimum $\hat{0}$ and maximum $\hat{1}$, and let $I \subseteq L$ be an order ideal of L. In the following theorem, we see how we can obtain information on $\mu_L(\hat{0}, \hat{1})$ in terms of I and its Möbius function. Actually, we will consider $\widehat{I} := I \cup \{\hat{1}\}$, that is I with the maximum $\hat{1}$ adjoined (we observe that clearly, by definition of an order ideal, $\hat{0} \in I$). The outcome is particularly relevant if we are interested in computational problems related to the Möbius function of the lattice, because a large ideal $I \subseteq L$ would allow us to give a more precise estimate of $\mu_L(\hat{0}, \hat{1})$. An example of application of Theorem 3.1.13 will be given in Chapter 5 to express the Möbius function of finite linear groups in terms of the ideal of reducible subgroups defined in Chapter 4.

Since it is so relevant, and even if it can be seen as a consequence of [3, Theorem 5.5], we prefer to provide a direct proof for Theorem 3.1.13 based on Hall's Theorem (Theorem 3.1.3).

Theorem 3.1.13. *Let L be a finite lattice with minimum $\hat{0}$ and maximum $\hat{1}$, and let $I \subseteq L$ be an order ideal of L. Let $\widehat{I} = I \cup \{\hat{1}\}$. Then*

$$\mu_L(\hat{0}, \hat{1}) = \mu_{\widehat{I}}(\hat{0}, \hat{1}) + \sum_{y \in L \setminus \widehat{I}} \mu_{\widehat{I}_{<y}}(\hat{0}, y) \cdot \mu_L(y, \hat{1}) \tag{3.11}$$

where $\widehat{I}_{<y} = \{x \in I \mid x < y\} \cup \{y\}$.

Remark. Notice that, if $\hat{1} \notin I$, then $I \neq L$ and (3.11) can also be written as

$$\mu_L(\hat{0}, \hat{1}) = \sum_{y \in L \setminus I} \mu_{\widehat{I}_{<y}}(\hat{0}, y) \cdot \mu_L(y, \hat{1}) \tag{3.12}$$

since $\widehat{I}_{<\hat{1}} = \widehat{I}$ and $\mu_L(\hat{1}, \hat{1}) = 1$.

Proof. Let $\mathcal{K}$ be the set of all chains from $\hat{0}$ to $\hat{1}$ in L, and let

$$\mathcal{K}_{\widehat{I}} = \{C \in \mathcal{K} \mid C \subseteq \widehat{I}\}$$

be the subset of $\mathcal{K}$ whose elements are the chains C contained in $\widehat{I}$. By Theorem 3.1.3,

$$\mu_L(\hat{0}, \hat{1}) = \sum_{C \in \mathcal{K}} (-1)^{\ell(C)} = \sum_{C \in \mathcal{K}_{\widehat{I}}} (-1)^{\ell(C)} + \sum_{C \in \mathcal{K} \setminus \mathcal{K}_{\widehat{I}}} (-1)^{\ell(C)}$$

$$= \mu_{\widehat{I}}(\hat{0}, \hat{1}) + \sum_{C \in \mathcal{K} \setminus \mathcal{K}_{\widehat{I}}} (-1)^{\ell(C)}. \tag{3.13}$$

We focus onto the second term on the right-hand side of (3.13). If $C \in \mathcal{K} \setminus \mathcal{K}_{\widehat{I}}$, then $C \setminus I$ is a chain in L and $C \setminus I$ has a minimum element $y \neq \hat{0}$. For each $y \in L \setminus \widehat{I}$ we set

$$\mathcal{K}_y = \{C \in \mathcal{K} \setminus \mathcal{K}_{\widehat{I}} \mid y \text{ is the minimum of } C \setminus I\}.$$

Then we define

$$\mathcal{J}_y = \{D \subseteq \widehat{I}_{<y} \mid D \text{ is a chain from } \hat{0} \text{ to } y \text{ in } \widehat{I}_{<y}\},$$

$$\mathcal{L}_y = \{E \subseteq L_{\geq y} \mid E \text{ is a chain from } y \text{ to } \hat{1} \text{ in } L_{\geq y}\}$$

and observe that there is a bijection

$$\beta : \mathcal{J}_y \times \mathcal{L}_y \to \mathcal{K}_y, \quad (D, E) \mapsto D \cup E.$$

between $\mathcal{J}_y \times \mathcal{L}_y$ and $\mathcal{K}_y$. Clearly the map β is well-defined and, if $C \in \mathcal{K}_y$, then C can be uniquely represented as an union $C = D \cup E$, with $D \in \mathcal{J}_y$ and $E \in \mathcal{L}_y$. In particular, $|C| = |D| + |E| - 1$ and therefore $\ell(C) = \ell(D) + \ell(E)$. Thus we have

$$\sum_{C \in \mathcal{K}_y} (-1)^{\ell(C)} = \sum_{(D,E) \in \mathcal{J}_y \times \mathcal{L}_y} (-1)^{\ell(D) + \ell(E)} = \sum_{D \in \mathcal{J}_y} (-1)^{\ell(D)} \cdot \sum_{E \in \mathcal{L}_y} (-1)^{\ell(E)}$$

$$= \mu_{\widehat{I}_{<y}}(\hat{0}, y) \cdot \mu_L(y, \hat{1})$$

where the last equality is given again by Theorem 3.1.3. Since

$$\sum_{C\in\mathcal{K}\setminus\mathcal{K}_{\widehat{I}}} (-1)^{\ell(C)} = \sum_{y\in L\setminus\widehat{I}} \sum_{C\in\mathcal{K}_y} (-1)^{\ell(C)},$$

we can write (3.13) as

$$\mu_L(\hat{0},\hat{1}) = \mu_{\widehat{I}}(\hat{0},\hat{1}) + \sum_{y\in L\setminus\widehat{I}} \mu_{\widehat{I}_{<y}}(\hat{0},y)\cdot\mu_L(y,\hat{1}).$$

□

Remark. In Theorem 3.1.13 we assume that L is a finite lattice because we need the existence of a maximum $\hat{1}$ and a minimum $\hat{0}$. But actually no other special property of lattices is required.

Finally, order ideals can be applied to determine the Möbius function of a finite distributive lattice.

Let L be a finite distributive lattice. Hence, by the fundamental Theorem 2.2.16, we have that $L \simeq \mathcal{O}(P)$ for the subposet $P = \mathrm{JI}(L)$ of join-irreducible elements of L. In particular, the isomorphism between L and $\mathcal{O}(P)$ is given by $f : L \to \mathcal{O}(\mathrm{JI}(L))$ so that

$$f(x) := \{a \in \mathrm{JI}(L) \mid a \le x\}.$$

By I_x we denote the ideal $f(x) \in \mathcal{O}(P)$, for all $x \in L$. So, for example,

$$I_{\hat{0}} \cong \{a \in \mathrm{JI}(L) \mid a \le \hat{0}\} = \emptyset \quad \text{and} \quad I_{\hat{1}} \cong \{a \in \mathrm{JI}(L) \mid a \le \hat{1}\} = \mathrm{JI}(L)$$

We remind that $\mathcal{O}(P)$ is ordered by inclusion.

Remark. For every interval $[I, I']$ of $\mathcal{O}(P)$ we have that

$$[I, I'] = \mathcal{O}(I' \setminus I)$$

where $I' \setminus I$ is regarded as an induced subposet of P. We also notice that every interval $[I, I']$ of $\mathcal{O}(P)$ is distributive and $I' \setminus I = \mathrm{JI}([I, I'])$. Let A be the set of atoms in the subposet $I' \setminus I$. Then, the join of all atoms in $[I, I']$ is the order ideal $I \cup A$. Therefore, I' is a join of atoms of $[I, I']$ if and only if the interval $[I, I']$ is a boolean lattice.

Let $x, y \in L$ so that $x \le y$. Then $I_x \subseteq I_y$ and we apply the above remark, together with Corollary 2.2.17 and (c) of Example 3.1.2, to say that

$$\mu_{\mathcal{O}(E)}(I_x, I_y) = \begin{cases} (-1)^{|I_y\setminus I_x|} = (-1)^{\ell([I_x,I_y])} & \text{if } [I_x, I_y] \text{ is boolean;} \\ 0 & \text{otherwise.} \end{cases}$$

Thanks to the isomorphism $f : L \to \mathcal{O}(\mathrm{JI}(L))$ sending x to I_x, we can conclude as follows.

Theorem 3.1.14. *Let L be a finite distributive lattice, and let $x \leq y$ in L. Then*

$$\mu_L(x,y) = \begin{cases} (-1)^{\ell([x,y])} & \text{if } [x,y] \text{ is boolean;} \\ 0 & \text{otherwise.} \end{cases}$$

In particular,

$$\mu_L(\hat{0},\hat{1}) = \begin{cases} (-1)^{|\mathrm{JI}(L)|} & \text{if } L \text{ is boolean;} \\ 0 & \text{otherwise.} \end{cases}$$

3.2 The Möbius function of groups

Let $\mathcal{L}(G)$ denote the subgroup lattice of a group G. Let G be a group such that $\mathcal{L}(G)$ is locally finite. The **Möbius function of** G is the Möbius function of its subgroup lattice, that is $\mu : \mathcal{L}(G) \times \mathcal{L}(G) \to \mathbb{Z}$ such that

$$\begin{cases} \mu(H,G) = 1 & \text{if } H = G \\ \sum_{H \leq K \leq G} \mu(K,G) = 0 & \text{if } H \neq G\,. \end{cases}$$

Usually the Möbius function of G is also written as a one-variable function

$$\mu_G : \mathcal{L}(G) \to \mathbb{Z}$$

such that

$$\begin{cases} \mu_G(H) = 1 & \text{if } H = G \\ \sum_{H \leq K \leq G} \mu_G(K) = 0 & \text{if } H \neq G\,. \end{cases}$$

So, the expression $\mu_G(\cdot)$ will simply substitute $\mu(\cdot, G)$ in the classical notation presented in §3.1. Clearly, all properties that we have shown for abstract posets and lattices have a group-theoretic counterpart.

Example 3.2.1.

(a) If we consider the classical Möbius function $\mu : \mathbb{N} \to \{0, \pm 1\}$, then we have that

$$\mu(n) = \mu_{\mathbb{Z}}(n\mathbb{Z}) = \mu_{C_n}(1)$$

for each cyclic group C_n of order $n \in \mathbb{N}$.

(b) Let G_1 and G_2 be two finite groups of coprime order. Let $H_1 \leq G_1$ and $H_2 \leq G_2$. Then

$$\mu(H_1 \times H_2, G_1 \times G_2) = \mu(H_1, G_1) \cdot \mu(H_2, G_2).$$

The subgroup lattice $\mathcal{L}(G)$ has a maximum and its coatoms correspond to the maximal subgroups of G. So, for $\mathcal{L}(G)$, Theorem 3.1.5 can be read as follows.

Proposition 3.2.2. *Let G be a group and let H be a subgroup of G of finite index. If $\mu_G(H) \neq 0$, then either $H = G$ or there exist maximal subgroups $M_1, \ldots, M_r$ of G such that $H = M_1 \cap \cdots \cap M_r$.*

Remark. It is not difficult to see that the converse of this fact is false. An easy counterexample is given by the following solvable group of order 20

$$G = C_4 \ltimes C_5 = \langle x, t \mid t^4 = x^5 = 1,\ x^t = x^2 \rangle,$$

whose maximal subgroups are $K := \langle t^2 \rangle \ltimes \langle x \rangle$ and $M_i := \langle tx^i \rangle$ for $i = 0, \ldots, 4$. Since $M_i \cap M_j = 1$ for $i \neq j$, we have that the trivial subgroup 1 is an intersection of maximal subgroups of G. By definition of μ_G, we notice that $\mu_G(K) = \mu_G(M_i) = -1$ (this is an obvious general property of maximal subgroups), and $\mu_G(K \cap M_i) = 1$ for all $i = 0, \ldots, 4$. The only other subgroup in the lattice $\mathcal{L}(G)$ is $C_5 = \langle x \rangle$, which has index 4 in G and is contained only in K. Therefore, $\mu_G(C_5) = 0$. An easy calculation shows that

$$\mu_G(1) = -\sum_{1 \neq H \leq G} \mu_G(H) = 0.$$

3.2.1 Some related questions

In [23] and [24], Kratzer and Thévenaz investigate, among others, conditions under which the converse of Proposition 3.2.2 holds for finite solvable groups and they can obtain many interesting results characterizing the Möbius function of such groups.

Example 3.2.3. Let G be a finite nilpotent group and let H be a proper subgroup of G. Then, $\mu_G(H) \neq 0$ is equivalent to saying that H is an intersection of maximal subgroups in G. Indeed, if H is an intersection of maximal subgroups of a finite nilpotent group G, then H is normal in G and $\mu(H, G) = \mu(1, G/H)$. Moreover, G/H is abelian because $G' \leq \Phi(G) \leq H$, where G' denotes the commutator of G and $\Phi(G)$ the Frattini subgroup. Hence $G/H \simeq \prod_{i=1}^{r} C_{p_i}^{d_i}$, where each $C_{p_i}^{d_i}$ is isomorphic to $\mathbb{F}_{p_i}^{d_i}$ with p_i prime. Therefore

$$\mu(H, G) = \prod_{i=1}^{r} (-1)^{d_i} p_i^{\binom{d_i}{2}}$$

by (b) in Example 3.2.1.

By using Crapo's Complement Theorem (Theorem 3.1.10), Kratzer and Thévenaz are even able to find a formula for $\mu_G(H)$ in all finite solvable groups.

Theorem 3.2.4 ([23], Théoréme 2.6)**.** *Let G be a finite solvable group. Let $1 = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G$ be a chief series of G, and $H \leq G$. We can consider the series*

$$H = G_nH \leq G_{n-1}H \leq \cdots \leq G_1H \leq G_0H = G \qquad (3.14)$$

whence we have the following series given by all distinct terms in (3.14)*:*

$$H = H_r < H_{r-1} < \cdots < H_1 < H_0 = G.$$

Let s_i be the number of complements of H_i in the interval $[H_{i+1}, G] \subseteq \mathcal{L}(G)$, for all $i = 1, \ldots, r-1$. Then

$$\mu(H, G) = (-1)^r \prod_{i=1}^{r-1} s_i \,.$$

Solvable groups represent an important source of problems related to the Möbius function. For instance, if G is a finite solvable groups, we can receive information on μ_G also from the Möbius function that can be defined on the poset $\Gamma(G)$ of conjugacy classes of subgroups in G.

Let G be a finite solvable group. Let $H, K \leq G$ and let $[H]$ and $[K]$ denote their conjugacy classes in G. We say that

$$[H] \leq [K] \text{ in } \Gamma(G) \quad \Leftrightarrow \quad H \leq K^g \text{ for some } g \in G$$

and we denote by $\lambda(H, G)$ the value $\mu_{\Gamma(G)}([H], [K])$ given by the Möbius function $\mu_{\Gamma(G)}$ of $\Gamma(G)$. Let μ be the usual Möbius function on the subgroup lattice $\mathcal{L}(G)$. Then, Pahlings shows in [33] that

$$\mu(H, G) = |N_{G'}(H) : G' \cap H| \cdot \lambda(H, G) \qquad (3.15)$$

extending a previous result contained in [19] for the trivial subgroup $1 \leq G$. It is observed in [33] that Equation (3.15) seems to be true for many non-solvable groups as well, but not for all of them. Some recent results, together with examples and counterexamples, are given in [14] by Dalla Volta and Zini. Moreover, Dalla Volta and Lucchini in [13] have recently generalized the Möbius function λ, by considering the Möbius function defined on the poset of the A-conjugacy classes of subgroups of G, where A is a subgroup of $\mathrm{Aut}(G)$. In this work, there are also some generalizations of Hall's results in [16], that we will now introduce as a further motivation.

Hall's interest in the Möbius function of finite simple groups is motivated by questions concerning the probability of generating groups. As in [16], let G be a finite group and let

$$\phi_k(G) := \#\{(g_1, \ldots, g_k) \in G^k \mid \langle g_1, \ldots, g_k \rangle = G\}$$

be the number of ordered k-tuples of elements in G which generate the group, so that we define

$$P(G,k) = \frac{\phi_k(G)}{|G|^k} \tag{3.16}$$

as the probability that k elements (independently chosen) generate G. Similarly, for all subgroups $H \leq G$, we set

$$\phi_k(H) = \#\{(g_1, \ldots, g_k) \in G^k \mid \langle g_1, \ldots, g_k \rangle = H\}\,.$$

Then

$$\sum_{H \leq G} \phi_k(H) = |G|^k$$

and by applying the Möbius inversion formula (Theorem 3.1.11) on the subgroup lattice $\mathcal{L}(G)$, we immediately obtain

$$\phi_k(G) = \sum_{H \leq G} |H|^k \mu(H,G)\,.$$

Thus, (3.16) can be written as

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

In [27], Mann proves that a similar result holds for all finitely generated profinite groups, as we explain in the following paragraph.

We recall that a **profinite group** is a compact, Hausdorff, and totally disconnected topological group (see [44] for more details about this definition). If G is a profinite group, then a subgroup of G is said to be **open** if it is also an open subset with respect to the topology of G. We denote by $H \leq_o G$ an open subgroup of G and we observe that the index of H in G is finite, since G is a compact topological group.

Let G be a profinite group and let X be a subset of G. We say that X (topologically) **generates** G if the subgroup $\langle X \rangle \leq G$ generated by X is dense in G. If there exists a finite subset X that generates G, then G is called **finitely generated**. We have the following interesting property for finitely generated profinite groups (see Proposition 2.5.1 in [34]).

Proposition 3.2.5. *Let G be a finitely generated profinite group. Then, for each $n \in \mathbb{N}$, the number of open subgroups of G of index n is finite.*

Remark. Moreover, it is worth recalling that an important theorem of Nikolov and Segal (Theorem 1.1 in [32]) states that in a finitely generated profinite group, every subgroup of finite index is open. It implies that the topology of a finitely generated profinite group is completely determined by its underlying abstract group structure.

Hence, if $\mathcal{L}(G)_o$ denotes the lattice of open subgroups of a finitely generated profinite group G, by Proposition 3.2.5 we have that $\mathcal{L}(G)_o$ is locally finite. Therefore, we can define recursively the Möbius function associated with the lattice $\mathcal{L}_o(G)$ of the open subgroups in G as

$$\mu_G : \mathcal{L}_o(G) \to \mathbb{Z}$$

such that

$$\begin{cases} \mu_G(H) = 1 & \text{if } H = G \\ \sum_{H \leq_o K \leq_o G} \mu_G(K) = 0 & \text{if } H <_o G\,. \end{cases} \tag{3.17}$$

Remark. Obviously, (3.17) generalizes the definition given for finite groups. A finite group G is endowed with the discrete topology, hence every subgroup of G is an open subgroup. Also in this case, $\mu_G(\cdot)$ has the same meaning as $\mu(\cdot, G)$.

If G is a finitely generated profinite group, then the direct product G^k admits a normalized Haar measure ν.

Notation. By $\overline{\langle g_1, \ldots, g_k\rangle} = G$ we mean that the elements $g_1, \ldots, g_k$ topologically generate G.

The set

$$\{(g_1, \ldots, g_k) \in G^k \mid \overline{\langle g_1, \ldots, g_k\rangle} = G\} \subset G^k$$

is a closed subset of G^k, hence it is measurable with respect to ν. We can define the probability $P(G, k)$ that k random ordered elements (chosen independently and with possible repetition in G) generate the whole group as

$$P(G, k) = \nu\left(\{(g_1, \ldots, g_k) \in G^k \mid \overline{\langle g_1, \ldots, g_k\rangle} = G\}\right).$$

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

Mann shows that for all $k \in \mathbb{N}$ we have

$$P(G, k) = \sum_{H \leq_o G} \frac{\mu_G(H)}{|G : H|^k}.$$

Moreover, he conjectures that if G is a PFG profinite group, then $P(G, k)$ can be interpolated in a natural way by an analytic function defined for all s in some complex right half-plane, and that this function can be expressed as

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

Since only subgroups with non-zero Möbius coefficient for G occur in the sum, the growth of their number could provide useful information for the convergence of the series $P_G(s)$. In particular, we need some specific notions of growth, as follows.

Notation. Let $b_n(G)$ denote the number of open subgroups H of index n in G satisfying $\mu_G(H) \neq 0$.

We say that $b_n(G)$ grows polynomially if $b_n(G) \leq n^t$ for some t independent of n. Similarly, $\mu_G(H)$ grows polynomially (in terms of the index) if $|\mu_G(H)|$ is bounded above by a polynomial function in the index of H in G, i.e. if $|\mu_G(H)| \leq |G : H|^u$ for some u independent of $H \leq_o G$.

Theorem 3.2.6. *Let G be a PFG group. The series $P(G,s)$ is absolutely convergent in some complex half-plane if and only if both $\mu_G(H)$ and $b_n(G)$ grow polynomially.*

Proof. Obviously if $P(G,s)$ converges absolutely, then $|\mu_G(H)|$ must be polynomially bounded by $|G : H|$. Since $\mu_G(H)$ is an integer, the subgroups of index n contribute at least $b_n(G)/n^s$ to the series of absolute values, so $b_n(G)$ also grows polynomially. Conversely, if $|\mu_G(H)|$ and $b_n(G)$ are polynomially bounded in terms of $|G : H|$ and n respectively, then there exists a large enough constant $C > 0$ such that for all s, with $\Re(s) \geq C$, the series is absolutely convergent. □

Conjecture 3.2.7 (Mann, [28]). *Let G be a PFG group. Then $|\mu_G(H)|$ is bounded by a polynomial function in the index $|G : H|$ and $b_n(G)$ grows at most polynomially in n.*

We recall that a group is **monolithic** if it contains a unique minimal normal subgroup.

Let G be a finitely generated profinite group.

Notation. We denote by $\Lambda(G)$ the set of finite monolithic groups L such that $\mathrm{soc}(L)$ is non-abelian and L is an epimorphic image of G.

If $L \in \Lambda(G)$, then let $b_n^*(L)$ be the number of subgroups $K \leq L$ such that $|L : K| = n$, $K\mathrm{soc}(L) = L$ and $\mu_L(K) \neq 0$.

Theorem 3.2.8 (Lucchini, [25]). *Let G be a PFG group. Then the following are equivalent.*

(*i*) *There exist two constants γ_1, γ_2 such that*

$$b_n(G) \leq n^{\gamma_1} \quad \text{and} \quad |\mu_G(H)| \leq |G : H|^{\gamma_2}$$

$\forall\, n \in \mathbb{N}$ *and for each open subgroup H of G.*

(*ii*) *There exist two constants c_1, c_2 such that*

$$b_n^*(L) \leq n^{c_1} \quad \text{and} \quad |\mu_L(X)| \leq |L : X|^{c_2}$$

$\forall\, L \in \Lambda(G)$, $\forall\, n \in \mathbb{N}$ *and for each $X \leq L$ with $L = X \,\mathrm{soc}\, L$.*

Thanks to Theorem 3.2.8, Mann's conjecture can be stated just in terms of finite monolithic groups with non-abelian socle.

Conjecture 3.2.9 (Lucchini, [25])**.** *For any positive integer $d \in \mathbb{N}$ there exists a constant c_d such that the following holds: if L is a d-generated finite monolithic group and* $\operatorname{soc} L$ *is non-abelian, then*

$$b_n^*(L) \leq n^{c_d} \quad \text{and} \quad |\mu_L(X)| \leq |L:X|^{c_d}$$

for each $n \in \mathbb{N}$ and each $X \leq L$ with $L = X \operatorname{soc} L$.

Actually, Conjecture 3.2.9 can be reduced to finite almost-simple groups. A finite group G is called **almost-simple** if there exists a non-abelian simple group S such that $S \leq G \leq \operatorname{Aut}(S)$.

Conjecture 3.2.10. *There exist two absolute constants γ_1 , γ_2 such that for each finite almost-simple group G we have*

(i) $|\mu(K,G)| \leq |G:K|^{\gamma_1}$ *for all $K \leq G$;*

(ii) $b_n(G) \leq n^{\gamma_2}$ *for all $n \in \mathbb{N}$.*

It means that if Conjecture 3.2.10 is true, then also Conjecture 3.2.9 is true. By Theorem 3.2.8, Mann's conjecture would be proven for all PFG profinite groups.

Now, the idea is to use the classification of finite simple groups to study Conjecture 3.2.10 for different classes of finite almost-simple groups.

In [10], Colombo and Lucchini proved that the alternating and symmetric groups ($\operatorname{Alt}(n)$, $\operatorname{Sym}(n)$, for $n \geq 5$) satisfy Conjecture 3.2.10, so that they obtained a proof of Mann's conjecture for finitely generated profinite groups with the property that all the non-abelian composition factors of every finite epimorphic image are permutation groups of alternating type. The argument in their proof is based on an application of Crapo's Closure Theorem (Theorem 3.1.9), as we will see at the beginning of Chapter 5.

Chapter 4

The reducible subgroup ideal

In this chapter we start to investigate properties of the Möbius function of finite classical groups, with emphasis on the linear case of $\mathrm{GL}(n, q)$. Most of the presented results are an original revision of some ideas and methods used by Shareshian in [38] to determine the number $\mu_G(1)$ for this kind of groups. We want to generalize Shareshian's outcome to any subgroup H in the subgroup lattice of G, with the purpose of finding estimations which can be helpful to study the conjectures of §3.2.

A central role is played by the reducible subgroup ideal, which is defined in §4.1 for a given subgroup $H \leq G$ and denoted by $\mathcal{I}_1(G, H)$. In §4.2 we see that it is possible to give an expression of its Möbius function by using only subsets of the lattice of H-invariant subspaces. This is interesting because it allows to exploit the computations that are presented in §4.3. In §4.4, attention is drawn to distributive lattices.

4.1 Definition of the ideal $\mathcal{I}_1(G, H)$ and notation

By a finite classical group we mean one of the linear, unitary, orthogonal or symplectic groups on finite vector spaces. General references for definitions of such groups are, for instance, [2], [6] and [42]. Our main results do not depend on the classical form defined on the vector space V, and if necessary, we focus on linear subgroups of $\mathrm{GL}(V)$. For this reason, we are not interested in recalling here all the properties related to classical forms on V. Nevertheless, it is important to remember that Kleidman and Liebeck in [21] give a very detailed description of finite classical groups and their subgroup structures, which are analysed starting from the fundamental results of Aschbacher in [1].

Let G be a finite classical group: Aschbacher establishes the existence of nine classes of maximal subgroups of G, denoted by $\mathcal{C}_i(G)$ for $i = 1, \ldots, 9$, such that each $H \leq G$ is contained in a subgroup $M \in \mathcal{C}_i(G)$, for some $i = 1, \ldots, 9$. The precise description of Aschbacher's classes for every finite classical group G is not easy and would be beyond the scope of this thesis, but a rough description is useful to understand what will follow.

So, if G is a finite classical group defined for a vector space $V \simeq \mathbb{F}_q^n$, we have 8 classes of *geometric* maximal subgroups of G:

- $\mathcal{C}_1(G)$: maximal reducible subgroups of G (stabilizers of subspaces);
- $\mathcal{C}_2(G)$: stabilizers of decompositions $V = \bigoplus_{j=1}^{t} V_j$, such that the dimension of all V_j is the same ($\dim(V_j) = a$ for all j. Hence, $n = at$);
- $\mathcal{C}_3(G)$: stabilizers of prime degree extension fields of F_q;
- $\mathcal{C}_4(G)$: stabilizers of tensor decompositions $V = V_1 \otimes V_2$;
- $\mathcal{C}_5(G)$: stabilizers of prime index subfields of $\mathbb{F}_q$;
- $\mathcal{C}_6(G)$: normalisers of symplectic-type r-groups with $\gcd(r, q) = 1$;
- $\mathcal{C}_7(G)$: stabilizers of decompositions $V = \bigotimes_{j=1}^{t} V_j$, such that the dimension of all V_j is the same ($\dim(V_j) = a$ for all j. Hence, $n = a^t$);
- $\mathcal{C}_8(G)$: classical subgroups.

The ninth class $\mathcal{C}_9(G)$ is the class of almost simple groups which do not lie in any of the other eight classes. Using the notation of [21], this class is usually referred to as the class $\mathcal{S}$.

In his doctoral thesis [38], Shareshian tries to figure out how he can compute $\mu(1, G)$ for several finite classical groups. His idea is to approximate $\mu(1, G)$ through a *good function* $f_{G,n,p}(u, 1)$, which allows to obtain a formula of the following type:

$$\mu(1, G(n,\, p^u)) = f_{G,n,p}(u, 1) + \sum_{K \in \mathcal{C}_9} \mu(1, K)\,. \tag{4.1}$$

Here $G = G(n, p^u)$ denotes a family of finite classical groups with the same defining classical form, which act in a natural way on the vector V of finite dimension n over the finite field of order $q = p^u$. If $\mathcal{C}_1, \ldots, \mathcal{C}_8, \mathcal{C}_9$ are the above described classes for the subgroups of G, then the function $f_{G,n,p}(u, 1)$ provides an estimate of $\mu(1, G)$ with respect to the contributions given by the subgroups of G which belong to the classes $\mathcal{C}_i$, for $i \in \{1, \ldots, 8\}$.

Actually, Shareshian's approach focuses on the first class $\mathcal{C}_1(G)$, that is the class of reducible subgroups of G. He studies in detail this class, and then tries to consider groups for which most of the other classes are empty.

In particular, the reducible subgroups of G contribute to $f_{G,n,p}(u, 1)$ through the computation of the Möbius function of

$$\widehat{\mathcal{I}}_1(G) = \{K \leq G \mid K \leq M \text{ for some } M \in \mathcal{C}_1(G)\} \cup \{G\}\,,$$

which is obtained by adjoining the maximum G to the order ideal

$$\mathcal{I}_1(G) = \{K \le G \mid K \le M \text{ for some } M \in \mathcal{C}_1(G)\}.$$

We observe that $\mathcal{I}_1(G) = \mathcal{L}(G)_{\le \mathcal{C}_1(G)}$ is the order ideal in $\mathcal{L}(G)$ generated by $\mathcal{C}_1(G)$, and its definition is independent of the classical form on V. We have that

$$\mu(1, G) = \mu_{\widehat{\mathcal{I}}_1(G)}(1, G) - \sum_{\substack{K<G \\ K \notin \mathcal{I}_1(G)}} \mu(1, K) \tag{4.2}$$

where

$$\mu_{\widehat{\mathcal{I}}_1(G)}(1, G) = - \sum_{K \in \mathcal{I}_1(G)} \mu_{\mathcal{I}_1(G)}(1, K) = - \sum_{K \in \mathcal{I}_1(G)} \mu(1, K)$$

by the general definition of an order ideal and by construction of $\mu_{\mathcal{I}_1(G)}$.

Shareshian is indeed able to obtain explicitly $f_{G,n,p}(u, 1)$ when many of the classes $C_i(G)$ are empty, for $i \ge 2$. Therefore, he considers orthogonal groups in odd characteristic and prime dimension, assuming some special condition on n. He also obtains some results when G is a linear group in odd characteristic and dimension 2. For some groups he even finds the exact value of $\mu(1, G)$.

Shareshian only considers the case of the trivial subgroup $H = \{1\}$, but his methods seem to suggest a general strategy for the computation of $\mu(H, G)$, for any non-trivial reducible subgroup $H \le G$. Since we are interested in all values of the Möbius function of G, and not only in $\mu(1, G)$, now we proceed from the following question to generalize the argument of Shareshian for all subgroups H of a finite classical group.

Question. *Can* (4.1) *and* (4.2) *be generalized to any subgroup* $H \neq \{1\}$*?*

The positive answer is immediate, as we can see with the following Definition 4.1.1 and Equation (4.3).

Let $H \le G$ and consider the lattice

$$\mathcal{L}(G)_{\ge H} = \{K \le G \mid H \le K\}$$

of subgroups containing H so that the intersection $\mathcal{C}_1(G) \cap \mathcal{L}(G)_{\ge H}$ is the set

$$\mathcal{C}_1(G, H) = \{\, \mathrm{stab}_G(W) \mid 0 < W < V \,,\, H \subseteq \mathrm{stab}_G(W) \,\}$$

of maximal reducible subgroups of G containing H. So, we can define an analogue of $\widehat{I}_1(G)$ as follows.

Definition 4.1.1. The **reducible subgroup ideal** in $\mathcal{L}(G)_{\geq H}$ is the order ideal generated by $\mathcal{C}_1(G,H)$. Namely,

$$\mathcal{I}_1(G,H) = \{K \leq G \mid H \leq K \leq M \text{ for some } M \in \mathcal{C}_1(G,H)\}$$

Remark. If H is reducible, then $H \in \mathcal{I}_1(G,H)$. Otherwise, if H is irreducible, clearly we have that $H \notin \mathcal{I}_1(G,H)$ and $\mathcal{I}_1(G,H) = \emptyset$ is the empty ideal.

Notation. If H is reducible, we set

$$\widehat{\mathcal{I}}_1(G,H) = \mathcal{I}_1(G,H) \cup \{G\}.$$

by adjoining the maximum G to $\mathcal{I}_1(G,H)$, which has minimum H. Otherwise, if H is irreducible, we set $\widehat{\mathcal{I}}_1(G,H) = \{H,G\}$ by adjoining the minimum H and the maximum G to the empty poset $\emptyset$.

Then, similarly to (4.2), we have

$$\mu(H,G) = \mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G) - \sum_{\substack{K \notin \mathcal{I}_1(G,H) \\ H \leq K < G}} \mu(H,K) \tag{4.3}$$

where $\mu_{\widehat{\mathcal{I}}_1(G,H)}$ is the Möbius function on $\widehat{\mathcal{I}}_1(G,H)$. So, if we are able to compute

$$\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G),$$

then we could try to study the sum over the other non-empty Aschbacher classes as suggested by Shareshian in his thesis.

In Chapter 4.5, we will see an example in this direction. Under some particular conditions, we will compute the value $\mu(H,G)$ for some particular subgroup H of G. A different use of the Möbius function of $\widehat{\mathcal{I}}_1(G,H)$ will be explained in Chapter 5 to study $\mu(H,G)$.

Definition 4.1.2. Let G be a finite classical group and let H be a subgroup of G. Let $\mathcal{I}_1(G,H)$ be the reducible subgroup ideal of $\mathcal{L}(G)$. We say that

$$\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G)$$

is **the Möbius number of** $\mathcal{I}_1(G,H)$, where $\widehat{\mathcal{I}}_1(G,H)$ is defined as above.

In particular, if H is irreducible, then $\widehat{\mathcal{I}}_1(G,H) = \{H,G\}$ and

$$\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G) = -1.$$

Therefore, the definition of the Möbius number of $\mathcal{I}_1(G,H)$ is interesting especially when H is a reducible subgroup of G.

Remark. It will be interesting to observe that our argument in §4.2 is again independent of the classical form on the vector space V. We will only fix a subgroup of $\mathrm{GL}(V)$ and then develop a purely combinatorial idea using the lattice $\mathcal{S}(V,H)$ of H-invariant subspaces of V.

4.2 The Möbius number of the ideal

We begin with fixing some more notation that will be used in this section. In particular, they allow us to prove Theorem 4.2.4, giving a "first approximation" of $\mu(H, G)$.

Notation. Remind that $\mathcal{S}(V, H)$ is the lattice of H-invariant subspaces of V. We define

$$\mathcal{S}(V, H)^* = \mathcal{S}(V, H) \setminus \{0, V\}\,.$$

Moreover, throughout the next sections, we will consider the following three sets:

(a) $\Psi(G, H) = \{X \subseteq \mathcal{C}_1(G, H) \mid \bigcap_{M\in X} M \neq H\}$;

(b) $\Psi(G, H)^{\complement} = \{Y \subseteq \mathcal{C}_1(G, H) \mid \bigcap_{M\in Y} M = H\}$;

(c) $\Psi'(G, H) = \{E \subseteq \mathcal{S}(V, H)^* \mid \bigcap_{W\in E} \mathrm{stab}_G(W) \neq H\}$.

for $H \leq G \leq \mathrm{GL}(V)$.

We also remark that $\emptyset \in \Psi(G, H)$ and $\emptyset \in \Psi'(G, H)$, but $\emptyset \notin \Psi(G, H)^{\complement}$.

The aim is to express the Möbius number of the ideal $\mathcal{I}_1(G, H)$ by using only the set $\Psi'(G, H)$, which is a set of H-invariant subspaces. This is useful because we would only use properties of $\mathcal{S}(V, H)$ to characterize the Möbius function of $\mathcal{L}(G)_{\geq H}$. We focus on some subgroup H, such that the lattice $\mathcal{S}(V, H)$ is well-known. In particular, we will consider more deeply the case when $\mathcal{S}(V, H)$ is distributive (see §4.4) or some particular case in Chapter 4.5.

We need a combinatorial lemma, that will be immediately applied to the above defined sets.

Lemma 4.2.1. *Let G be a finite group and H a subgroup of G. Let G act on a finite set X, so that for all $x \in X$*

$$G_x = \{g \in G \mid x^g = x\}$$

is the stabilizer of x in G. Let $X' \subseteq X$ be a subset such that $H \leq G_x$ for all $x \in X'$. Set

- $\mathcal{G} = \{G_x \mid x \in X'\}$;
- $\mathcal{R} = \{E \subseteq \mathcal{G} \mid \bigcap_{K\in E} K \neq H\}$;
- $\mathcal{S} = \{Q \subseteq X' \mid \bigcap_{x\in Q} G_x \neq H\}$.

Then

$$\sum_{E\in\mathcal{R}} (-1)^{|E|} = \sum_{Q\in\mathcal{S}} (-1)^{|Q|}\,.$$

Proof. If Q is a subset of X', then let $\mathcal{G}_Q = \{G_x \mid x \in Q\}$. For every $E \in \mathcal{R}$, we define

$$\mathcal{S}_E = \{Q \in \mathcal{S} \mid E = \mathcal{G}_Q\}.$$

Then

$$\mathcal{S} = \bigsqcup_{E \in \mathcal{R}} \mathcal{S}_E$$

is the disjoint union of all the $\mathcal{S}_E$, and it suffices to show that for each $E \in \mathcal{R}$ we have

$$(-1)^{|E|} = \sum_{Q \in \mathcal{S}_E} (-1)^{|Q|}.$$

Fix $E \in \mathcal{R}$ and observe that

$$Q \in \mathcal{S}_E \quad \Leftrightarrow \quad Q = \bigsqcup_{K \in E} Q_K,$$

where $Q_K = \{x \in Q \mid G_x = K\}$. Then define, for each $K \in E$,

$$X'_K = \{x \in X' \mid G_x = K\} \subseteq X',$$

and notice that $Q_K \subseteq X'_K$. So, by using the principle of inclusion-exclusion and the fact that the Q_K are non-empty and can be chosen independently, we get

$$\sum_{Q \in \mathcal{S}_E} (-1)^{|Q|} = \prod_{K \in E} \underbrace{\left(\sum_{\emptyset \neq Q_K \subseteq X'_K} (-1)^{|Q_K|} \right)}_{=-1} = \prod_{K \in E} (-1) = (-1)^{|E|}.$$

□

As an immediate consequence, we find out a link between $\Psi(G,H)$ ad $\Psi'(G,H)$.

Proposition 4.2.2. *Let V be a vector space of finite dimension over $\mathbb{F}_q$. Let $H \leq G \leq \mathrm{GL}(V)$. Then we have that*

$$\sum_{E \in \Psi'(G,H)} (-1)^{|E|} = \sum_{\mathcal{X} \in \Psi(G,H)} (-1)^{|\mathcal{X}|}. \tag{4.4}$$

Proof. We consider the natural action of G on V. Then, by lemma 4.2.1, the equality is an immediate consequence of the definitions of $\mathcal{S}(V,H)^*$, $\mathcal{C}_1(G,H)$, $\Psi(G,H)$ and $\Psi'(G,H)$. □

On the other hand, if we try to compute

$$\sum_{Y \in \Psi(G,H)^{\complement}} (-1)^{|Y|},$$

we realize that, by Crosscut Theorem (Theorem 3.1.6), this sum is the link to the Möbius number of $\mathcal{I}_1(G,H)$.

Proposition 4.2.3. *Let V be a vector space of finite dimension over $\mathbb{F}_q$. Let $H \leq G \leq \mathrm{GL}(V)$. Then we have that*

$$\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G) = \sum_{Y \in \Psi(G,H)^{\complement}} (-1)^{|Y|}. \tag{4.5}$$

Proof. In order to use Theorem 3.1.6, we need a finite lattice L and the set of all coatoms in L. We observe that $\widehat{\mathcal{I}}_1(G,H)$ is a sublattice of $\mathcal{L}(G)_{\geq H}$, because the subgroup generated by two subgroups $K_1, K_2 \in \mathcal{I}_1(G,H)$ is either in $\mathcal{I}_1(G,H)$ or equal to G. Hence, $\widehat{\mathcal{I}}_1(G,H)$ is a finite lattice, whose coatoms are the subgroups in $\mathcal{C}_1(G,H)$. Since

$$\Psi(G,H)^{\complement} = \{Y \subseteq \mathcal{C}_1(G,H) \mid Y \neq \emptyset \text{ and } \bigcap_{M \in Y} M = H\},$$

by Theorem 3.1.6 we immediately obtain (4.5). □

Remark. We observe that $\Psi(G,H) \cup \Psi(G,H)^{\complement}$ is the power set of $\mathcal{C}_1(G)$. Since for every finite set A of cardinality $n > 0$ we have

$$\sum_{S \subseteq A} (-1)^{|S|} = \sum_{k=0}^{n} \binom{n}{k} (-1)^k = (1-1)^n = 0,$$

then clearly

$$\sum_{X \in \Psi(G,H)} (-1)^{|X|} + \sum_{Y \in \Psi(G,H)^{\complement}} (-1)^{|Y|} = 0. \tag{4.6}$$

If we put together equations (4.4), (4.5), and (4.6), we obtain an expression of the Möbius number of $\mathcal{I}_1(G,H)$ by subsets of $\mathcal{S}(V,H)$.

Theorem 4.2.4. *Let V be a vector space of finite dimension over $\mathbb{F}_q$. Let $H \leq G \leq \mathrm{GL}(V)$. Then*

$$-\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G) = \sum_{E \in \Psi'(G,H)} (-1)^{|E|}. \tag{4.7}$$

Proof. By (4.6), we have

$$\sum_{\mathcal{X} \in \Psi(G,H)} (-1)^{|\mathcal{X}|} = - \sum_{\mathcal{Y} \in \Psi(G,H)^{\complement}} (-1)^{|\mathcal{Y}|}.$$

Then, by Lemma 4.2.2 and Lemma 4.2.3,

$$\sum_{E \in \Psi'(G,H)} (-1)^{|E|} = \sum_{\mathcal{X} \in \Psi(G,H)} (-1)^{|\mathcal{X}|} = - \sum_{\mathcal{Y} \in \Psi(G,H)^{\complement}} (-1)^{|\mathcal{Y}|}$$

$$= -\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G).$$

□

The sum

$$\sum_{E\in\Psi'(G,H)} (-1)^{|E|}$$

coming from (4.6) can be exploited to estimate the Möbius function of G. In the following section we shall develop methods to obtain information for $\mu(H,G)$, at least for some specific subgroup $H \leq G$ such that the lattice $\mathcal{S}(V,H)$ is known.

4.3 Some relevant sets of H-invariant subspaces

According to what we have mentioned in the last part of §4.2, we want to introduce some special subsets of H-invariant subspaces.

First, we recall that by Theorem 4.2.4 we have

$$-\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G) = \sum_{E\in\Psi'(G,H)} (-1)^{|E|} \tag{4.8}$$

where

$$\Psi'(G,H) = \{E \subseteq \mathcal{S}(V,H)^* \mid \bigcap_{W\in E} \mathrm{stab}_G(W) \neq H\}\,.$$

In order to simplify the computation in (4.8), we look for some subset $S \subseteq \Psi'(G,H)$, so that the sum can be split into the following two parts:

$$\sum_{E\in\Psi'(G,H)} (-1)^{|E|} = \sum_{E\in\Psi'(G,H)\cap S} (-1)^{|E|} + \sum_{E\in\Psi'(G,H)\setminus S} (-1)^{|E|}\,.$$

In §4.3.1 and §4.3.2 of this section, we will introduce the following two particular kinds of sets of H-invariant subspaces:

- $N(V,H)$: the collection of non-spanning sets in $\mathcal{S}(V,H)$;
- $D(V,H)$: the collection of decomposing sets in $\mathcal{S}(V,H)$.

Their union will be denoted by

$$\Gamma(V,H) = N(V,H) \cup D(V,H)\,.$$

In §4.4 we will be interested in some particular case for which it will be useful to split the sum in (4.8) in the following way:

$$-\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G) = \sum_{E\in\Psi'(G,H)\cap\Gamma(V,H)} (-1)^{|E|} + \sum_{E\in\Psi'(G,H)\setminus\Gamma(V,H)} (-1)^{|E|}\,.$$

We will show that, if the lattice $\mathcal{S}(V,H)$ is distributive and it has prime rank, then

$$\sum_{E\in\Psi'(G,H)\setminus\Gamma(V,H)} (-1)^{|E|} = 0. \tag{4.9}$$

It may be interesting to observe that, whenever the condition

$$\Gamma(V,H) \subseteq \Psi'(G,H) \tag{4.10}$$

is satisfied, then

$$-\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G) = \sum_{E\in\Psi'(G,H)} (-1)^{|E|} = \sum_{E\in\Gamma(V,H)} (-1)^{|E|} \,.$$

In Theorem 4.4.5, we will show that

$$\sum_{E\in\Gamma(V,H)} (-1)^{|E|} = 0$$

for all subgroups H such that $\mathcal{S}(V,H)$ is distributive.

In Chapter 5, moreover, we will identify a class of subgroups such that

$$\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G) = 0.$$

4.3.1 Non-spanning sets

We start with non-spanning sets of V. As we are considering, for some reducible subgroup $H \leq \mathrm{GL}(V)$, the lattice $\mathcal{S}(V,H)$ of H-invariant subspaces in V, every subspace is H-invariant, unless otherwise stated.

Notation. Let $H \leq \mathrm{GL}(V)$ and let $X \in \mathcal{S}(V,H)$ be a H-invariant subspace of V. Since the context is clear, in the sense that we consider only H-invariant subspaces, we denote by $\mathcal{S}(X,H)$ the principal order ideal $\mathcal{S}(V,H)$ generated by T, instead of writing every time

$$\mathcal{S}(V,H)_{\leq X} = \{W \in \mathcal{S}(V,H) \mid W \leq X\}.$$

Moreover, we have $\mathcal{S}(X,H)^* = \mathcal{S}(X,H) \setminus \{0,X\}$. Clearly, if $X = V$, the lattice $\mathcal{S}(X,H)$ coincides with $\mathcal{S}(V,H)$.

Definition 4.3.1. Let V be a vector space and $H \leq \mathrm{GL}(V)$. Let $X \in \mathcal{S}(V,H) \setminus \{0\}$. We say that a set $E \subseteq \mathcal{S}(X,H)$ is **non-spanning** for X if

$$\sum_{W\in E} W \neq X \,.$$

Notation. The collection of all non-spanning sets for X is denoted by

$$N(X,H) = \{E \subseteq \mathcal{S}(X,H)^* \mid \sum_{W\in E} W \neq X\}\,,$$

where we exclude the possibility for subspace in E to be the zero-space 0. We also observe that for us the empty subset $\emptyset$ is non-spanning, hence $\emptyset \in N(X,H)$.

We see that, by using the Crosscut Theorem (Theorem 3.1.6), it is quite easy to compute

$$\sum_{E \in N(X,H)} (-1)^{|E|} \,.$$

Proposition 4.3.2. *Let V be a vector space of finite dimension over $\mathbb{F}_q$, and let $H \leq \mathrm{GL}(V)$. Let $X \in \mathcal{S}(V,H) \setminus \{0\}$. Then*

$$\sum_{E \in N(X,H)} (-1)^{|E|} = -\mu_{\mathcal{S}(X,H)}(0,X) \tag{4.11}$$

where $\mu_{\mathcal{S}(X,H)}$ denotes the Möbius function of $\mathcal{S}(X,H)$.

Proof. The equality follows immediately from the application of the dual version of Theorem 3.1.6. We consider the lattice $\mathcal{S}(X,H)$, whose atoms are contained in $\mathcal{S}(X,H)^*$. But $0 \notin \mathcal{S}(X,H)^*$, and 0 is the minimum of $\mathcal{S}(X,H)$. Therefore, we have

$$\mu_{\mathcal{S}(X,H)}(0,X) = \sum_{F \in N(X,H)^{\complement}} (-1)^{|F|} \tag{4.12}$$

where $N(X,H)^{\complement} = \{F \subseteq \mathcal{S}(X,H)^* \mid \sum_{W \in F} W = X\}$ is the collection of spanning sets for X in $\mathcal{S}(X,H)^*$. Consequently,

$$-\mu_{\mathcal{S}(X,H)}(0,X) = \sum_{E \in N(X,H)} (-1)^{|E|} \,.$$

□

In particular, for $X = V$ we have

Corollary 4.3.3. *Let V be a vector space of finite dimension over $\mathbb{F}_q$, and let $H \leq \mathrm{GL}(V)$. Then*

$$\sum_{E \in N(V,H)} (-1)^{|E|} = -\mu_{\mathcal{S}(V,H)}(0,V)\,,$$

Remark. If $H = 1$, clearly $\mathcal{S}(V,H) = \mathcal{S}_V$ that is the subspace lattice of V. We have that

$$\sum_{E \in N(V,1)} (-1)^{|E|} = -\mu_{\mathcal{S}_V}(0,V) = (-1)^{n+1} q^{\binom{n}{2}}\,,$$

4.3.2 Decomposing sets

As regards to $D(V,H)$, we do not have such an immediate way to compute

$$\sum_{E\in D(V,H)} (-1)^{|E|}$$

as in the case of $N(V,H)$. In this section we gather some general information, that we shall use under additional assumptions in §4.4 or in Chapter 4.5.

Let V be a vector space and $H \leq \mathrm{GL}(V)$. Let $X \in \mathcal{S}(V,H)\setminus\{0\}$. A **proper direct decomposition** of H-invariant subspaces for X is given by a subset $\Delta \subseteq \mathcal{S}(X,H)^*$ of proper subspaces of X such that

$$\sum_{T\in\Delta} T = X$$

and

$$\forall\, T_1, T_2 \in \Delta \quad T_1 \cap T_2 = 0\,.$$

We write

$$X = \bigoplus_{T\in\Delta} T\,.$$

Remark. Since $\mathcal{S}(X,H)^* = \mathcal{S}(X,H)\setminus\{0,X\}$, we observe that $|\Delta| \geq 2$.

We will denote by $\mathfrak{D}(X,H)$ the collection of all proper direct decompositions of H-invariant subspaces for X, namely

$$\mathfrak{D}(X,H) = \left\{ \Delta \subseteq \mathcal{S}(X,H)^* \;\middle|\; X = \bigoplus_{T\in\Delta} T \right\}.$$

Notation. With some abuse of notation, if $\Delta = \{S_1,\dots,S_r\} \in \mathfrak{D}(V,H)$ is a finite proper direct decomposition of H-invariant subspaces for $X \in \mathcal{S}(V,H)\setminus\{0\}$, we could write sometimes

$$\Delta : X = \bigoplus_{j=1}^{r} S_j \in \mathfrak{D}(X,H)\,.$$

Observe also, in particular, that we do not care about the order in which we write the S_j.

We give now the following relevant definition.

Definition 4.3.4. Let V be a vector space and $H \leq \mathrm{GL}(V)$. Let $X \in \mathcal{S}(V,H)\setminus\{0\}$. A subset E of $\mathcal{S}(X,H)^*$ is said to be a (proper) **decomposing set** of H-invariant subspaces for X if it satisfies the two following conditions:

(*i*) $\sum_{T\in E} T = X$;

(*ii*) there exists a proper direct decomposition $\Delta \in \mathfrak{D}(X, H)$ such that

$$\forall T \in E \quad \exists S \in \Delta : \quad T \subseteq S.$$

The collection of all decomposing sets of H-invariant subspaces for $X \in \mathcal{S}(V, H) \setminus \{0\}$ is denoted by

$$D(X, H) = \{E \subseteq \mathcal{S}(X, H)^* \mid E \text{ is a decomposing set for } X\}.$$

Remark. Let E be a decomposing set of H-invariant subspaces for X and let $\Delta \in \mathfrak{D}(X, H)$ be so that for every $T \in E$ there exists $S \in \Delta$ with $T \subseteq S$. Fix $S_0 \in \Delta$, and set

$$F = \{W \in E \mid T \subseteq S_0\}.$$

Then $S_0 = \sum_{W \in F} W$.

If V is a vector space of finite dimension over $\mathbb{F}_q$, then for every $X \in \mathcal{S}(V, H) \setminus \{0\}$ the cardinality $|D(X, H)|$ is finite, and we have $|E| < \infty$ for every $E \in D(X, H)$. In this case, we want to find a different way to express

$$\sum_{E \in D(X,H)} (-1)^{|E|}.$$

First, we can compare two direct decompositions $\Delta_1, \Delta_2 \in \mathfrak{D}(X, H)$ by saying that Δ_1 is **finer** than Δ_2 if

$$\forall S \in \Delta_1 \quad \exists R \in \Delta_2 \quad \text{such that} \quad S \subseteq R.$$

Lemma 4.3.5. *Let V be a vector space of finite dimension over $\mathbb{F}_q$, and let $H \leq \mathrm{GL}(V)$. Let $X \in \mathcal{S}(V, H) \setminus \{0\}$. Let $E = \{T_1, \ldots, T_k\} \subseteq \mathcal{S}(X, H)^*$ such that $E \in D(X, H)$. Then there exists a unique finest proper direct decomposition $X = \bigoplus_{j=1}^{r} S_j \in \mathfrak{D}(X, H)$ such that each T_i is contained in some S_j.*

Proof. Let $X = \bigoplus_{j=1}^{r_1} S_j$ and $X = \bigoplus_{l=1}^{r_2} S'_l$ be two direct decompositions in $\mathfrak{D}(V, H)$ such that each T_i is contained in some S_j and in some S'_l.
Let $I = \{(j, l) : S_j \cap S'_l \neq 0\}$ (obviously $|I| < \infty$). Since $\sum_{i=1}^{k} T_i = V$ and each T_i is contained in $S_j \cap S'_l$ for some $(j, l) \in I$, we have

$$X = \bigoplus_{(j,l) \in I} S_j \cap S'_l \in \mathfrak{D}(V, H).$$

Since $\mathcal{S}(X, H)$ is finite, the result follows immediately. □

As a direct consequence of Lemma 4.3.5, we have the following.

Proposition 4.3.6. *Let V be a vector space of finite dimension over $\mathbb{F}_q$, and let $H \le \mathrm{GL}(V)$. Let $X \in \mathcal{S}(V,H) \setminus \{0\}$. Then there exists a surjective function*

$$\partial_X : D(X,H) \to \mathfrak{D}(X,H)$$

that maps each $E \in D(X,H)$ into the finest proper direct decomposition Δ such that every $T \in E$ is contained in some $S \in \Delta$.

Notation. So, using the notation of Preposition 4.3.6, for all $E \in D(X,H)$ we denote by $\partial_X(E)$ the finest proper direct decomposition Δ such that every $T \in E$ is contained in some $S \in \Delta$. If the context is clear, we can just write $\partial(E)$. There is an equivalence relation on the set $D(X,H)$ induced by ∂_X, whose equivalence classes are

$$D(X,H)_\Delta = \{E \in D(X,H) \mid \partial_X(E) = \Delta\} = \partial_X^{-1}(\Delta).$$

for all $\Delta \in \mathfrak{D}(V,H)$. Then

$$D(X,H) = \bigsqcup_{\Delta \in \mathfrak{D}(V,H)} D(X,H)_\Delta\,.$$

So we can write

$$\sum_{E \in D(X,H)} (-1)^{|E|} = \sum_{\Delta \in \mathfrak{D}(X,H)} \left(\sum_{E \in D(X,H)_\Delta} (-1)^{|E|} \right)$$

where

$$\sum_{E \in D(X,H)_\Delta} (-1)^{|E|} = \sum_{\substack{E \in D(X,H) \\ \partial(E) = \Delta}} (-1)^{|E|}\,.$$

Proposition 4.3.7. *Let V be a vector space of finite dimension over $\mathbb{F}_q$, and $H \le \mathrm{GL}(V)$. Let $X \in \mathcal{S}(V,H) \setminus \{0\}$. Let $\Delta : X = \bigoplus_{j=1}^r S_j$ be any proper decomposition of X such that $\Delta \in \mathfrak{D}(X,H)$. Then*

$$\sum_{E \in D(X,H)_\Delta} (-1)^{|E|} = (-1)^r \prod_{j=1}^{r} \sum_{F \in \Gamma(S_j,H)} (-1)^{|F|} \tag{4.13}$$

where $\Gamma(S_j,H) = N(S_j,H) \cup D(S_j,H)$.

Proof. Fix $E = \{T_1, \dots, T_k\} \in D(X,H)$ with $\partial_X(E) = \Delta$.
For each $j \in \{1, \dots, r\}$ set

$$E_j = \{T_i \mid T_i \le S_j\}.$$

Since $E \in D(X,H)$, we have that the subspaces in E_j span S_j. Therefore $E_j \notin N(S_j,H)$. Moreover:

- by definition, if E_j contains some $V_i = S_j$, then $E_j \notin D(S_j, H)$;
- if E_j does not contain S_j, then $E_j \notin D(S_j, H)$ as well, since otherwise there is a finer proper direct decomposition of X in $\mathfrak{D}(X, H)$ such that each V_i is contained in some addend.

So $E_j \notin \Gamma(S_j, H)$.
Conversely, if for each $j \in \{1, \ldots, r\}$ we choose a collection $F_j \subseteq \mathcal{S}_{S_j}(H) \setminus \{0\}$ of non-trivial subspaces of S_j fixed by H, such that

$$F_j \notin \Gamma(S_j, H)\,,$$

then $F := \bigcup_{j=1}^r F_j\,,\ \ F \in D(X, H)$ and satisfies $\partial_X(F) = \Delta$. Notice that the F_j can be chosen independently of each other.
So we have $|E| = |E_1| + \ldots + |E_r|$ and

$$\begin{aligned}
\sum_{E \in D(X,H)_\Delta} (-1)^{|E|} &= \sum_{\substack{E_1 \subseteq \mathcal{S}_{S_1}(H)\setminus\{0\}, \ldots, E_r \subseteq \mathcal{S}_{S_r}(H)\setminus\{0\} \\ E_1 \notin \Gamma(S_1, H), \ldots, E_r \notin \Gamma(S_r, H)}} (-1)^{|E_1| + \ldots + |E_r|} \\
&= \sum_{\substack{E_1 \subseteq \mathcal{S}_{S_1}(H)\setminus\{0\}, \ldots, E_r \subseteq \mathcal{S}_{S_r}(H)\setminus\{0\} \\ E_1 \notin \Gamma(S_1, H), \ldots, E_r \notin \Gamma(S_r, H)}} (-1)^{|E_1|} \cdot \ldots \cdot (-1)^{|E_r|} \\
&= \prod_{j=1}^r \sum_{\substack{F \subseteq \mathcal{S}_{S_j}(H)\setminus\{0\} \\ F \notin \Gamma(S_j, H)}} (-1)^{|F|}\,.
\end{aligned}$$

Since $\mathcal{S}_{S_j}(H) \setminus \{0\}$ is a finite a set,

$$\sum_{\substack{F \subseteq \mathcal{S}_{S_j}(H)\setminus\{0\} \\ F \notin \Gamma(S_j, H)}} (-1)^{|F|} = - \sum_{F \in \Gamma(S_j, H)} (-1)^{|F|}$$

and finally we obtain (4.13). □

In particular, for $X = V$, we have the following.

Corollary 4.3.8. *Let $\Delta : V = \bigoplus_{j=1}^r S_j$ be any proper decomposition of V such that $\Delta \in \mathfrak{D}(V, H)$. Then*

$$\sum_{E \in D(V,H)_\Delta} (-1)^{|E|} = (-1)^r \prod_{j=1}^r \sum_{F \in \Gamma(S_j, H)} (-1)^{|F|}\,.$$

where $\Gamma(S_j, H) = N(S_j, H) \cup D(S_j, H)$.

Lastly, we want to define here the rank of a direct decomposition, in a general context. It will be particularly useful in §4.4, where we assume that the lattice $\mathcal{S}(V, H)$ is distributive.

Definition 4.3.9. Let V be a vector space of finite dimension over $\mathbb{F}_q$. Let $H \leq G = \mathrm{GL}(V)$ and let $X \in \mathcal{S}(V,H) \setminus \{0\}$. Let $\Delta \in \mathfrak{D}(X,H)$ be a proper direct decomposition of H-invariant subspaces for X. We say that Δ has **rank** k, for $k \in \mathbb{N}$, if

$$k = \max\{\,\mathrm{rk}(S) \mid S \in \Delta\}$$

where $\mathrm{rk}(S)$ denotes the rank of each $S \in \Delta$ in the modular lattice $\mathcal{S}(X,H)$. We will write $\mathrm{rk}_{\mathfrak{D}}(\Delta)$ to denote the rank of Δ.

Remark. Observe that for a proper direct decomposition $\Delta \in \mathfrak{D}(X,H)$ we have $\mathrm{rk}_{\mathfrak{D}}(\Delta) < \mathrm{rk}(X)$, since $\mathrm{rk}(S) < \mathrm{rk}(X)$ for all $S \in \Delta$.

Example 4.3.10. If $\mathrm{rk}_{\mathfrak{D}}(\Delta) = 1$ for some $\Delta \in \mathfrak{D}(X,H)$, then X is a direct sum of subspaces of rank 1 in $\mathcal{S}(X,H)$. This means that every $T \in \Delta$ is an atom of $\mathcal{S}(X,H)$.

Remark. In general, there could be more than one proper direct decomposition in $\mathfrak{D}(X,H)$ of rank 1. As an example, take $X = V \simeq \mathbb{F}_q^n$ and $H = 1 \leq \mathrm{GL}(V)$. It could also happen that there is no proper direct decomposition of rank 1. For instance, take $X = V$ and H a maximal parabolic subgroup (i.e. the stabiliser of a complete flag, that will be also defined in §5.3.1).

In the situation presented in the following proposition, we have exactly one proper direct decomposition of rank 1 in $\mathfrak{D}(X,H)$. It is a direct consequence of Corollary 2.2.17 and it will be used in section §4.4, for the computation of $\sum_{E \in D(V,H)} (-1)^{|E|}$ when the lattice $\mathcal{S}(V,H)$ is boolean.

Proposition 4.3.11. *Let V be a vector space of finite dimension over $\mathbb{F}_q$, and let $H \leq \mathrm{GL}(V)$. Let $X \in \mathcal{S}(V,H) \setminus \{0\}$ and assume that the sublattice $\mathcal{S}(X,H)$ is distributive. If there exists $\Delta \in \mathfrak{D}(X,H)$ with $\mathrm{rk}_{\mathfrak{D}}(\Delta) = 1$, then $\mathcal{S}(X,H)$ is boolean and Δ is the unique proper direct decomposition of H-invariant subspaces for X of rank* 1.

4.3.3 Antichains

Now we concentrate on the term

$$\sum_{E \in \Psi'(G,H) \setminus \Gamma(V,H)} (-1)^{|E|} \tag{4.14}$$

which is relevant if we are considering $-\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G)$ written as

$$-\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G) = \sum_{E \in \Psi'(G,H) \cap \Gamma(V,H)} (-1)^{|E|} + \sum_{E \in \Psi'(G,H) \setminus \Gamma(V,H)} (-1)^{|E|}$$

Antichains play an important role. The next results will be useful in §4.4 and in Chapter 4.5.

Definition 4.3.12. Let V be a vector space over $\mathbb{F}_q$. Let $H \leq G \leq \mathrm{GL}(V)$. Let $E \in \Psi'(G,H) \setminus \Gamma(V,H)$. Then

$$A_E = \{T \in E \mid T \text{ is maximal in } E\}$$

is the set of elements of E which are maximal in E with respect to the order relation induced by $\mathcal{S}(V,H)$.

Proposition 4.3.13. *Let V be a vector space over $\mathbb{F}_q$. Let $H \leq G \leq \mathrm{GL}(V)$. Let $E \in \Psi'(G,H) \setminus \Gamma(V,H)$. Then A_E is an antichain in $\mathcal{S}(V,H)^*$ and $A_E \in \Psi'(G,H) \setminus \Gamma(V,H)$.*

Proof. By definition, the elements of A_E are maximal subspaces in E. Then T_1 is not contained in T_2 for any T_1, T_2 in A_E. Since $A_E \subseteq E$, we have that if $g \in G$ stabilizes all elements of E, then g stabilizes all elements of A_E. So, by definition, $A_E \in \Psi'(G,H)$. Moreover we notice that

$$\begin{cases} A_E \in N(V,H) & \Leftrightarrow \quad E \in N(V,H) \\ A_E \in D(V,H) & \Leftrightarrow \quad E \in D(V,H). \end{cases}$$

Therefore $A_E \in \Gamma(V,H)$ if and only if $E \in \Gamma(V,H)$. □

If V is a vector space over $\mathbb{F}_q$ and $G \leq \mathrm{GL}(V)$, we denote by

$$\mathcal{A} = \{A \in \Psi'(G,H) \setminus \Gamma(V,H) \mid A \text{ is antichain in } \mathcal{S}(V,H)^*\}$$

the set of antichains in $\mathcal{S}(V,H)^*$ which lie in $\Psi'(G,H) \setminus \Gamma(V,H)$

Proposition 4.3.14. *Let V be a vector space over $\mathbb{F}_q$. Let $H \leq G \leq \mathrm{GL}(V)$. Then*

$$\sum_{E \in \Psi'(G,H) \setminus \Gamma(V,H)} (-1)^{|E|} = \sum_{A \in \mathcal{A}} \sum_{A_E = A} (-1)^{|E|}$$

Proof. This is an immediate consequence of the definition of $\mathcal{A}$ and follows from the fact that

$$E \in \Psi'(G,H) \setminus \Gamma(V,H) \Leftrightarrow A_E \text{ is antichain } \& \ A_E \in \Psi'(G,H) \setminus \Gamma(V,H),$$

as showed in proposition 4.3.13. □

Thus, by Proposition 4.3.14, the study of the behaviour of sums over antichains in $\mathcal{S}(V,H)$ seems interesting to estimate (4.14). Here below, Proposition 4.3.15 and the following corollary state a nice property, that will be applied to prove Lemma 4.3.17, which is the main result of this focus on antichains. We are assuming that V, G, H, $\mathcal{A}$ are the same as above.

Proposition 4.3.15. *Let* $A = \{X_1, \ldots, X_k\} \in \mathcal{A}$ *and let* $E \in \Psi'(G,H) \setminus \Gamma(V,H)$ *, so that* $A_E = A$ *.*
Assume that there exist $i \in \{1, \ldots, k\}$ *and* $J \subseteq \{1, \ldots, k\}$ *such that*

$$0 < X := X_i \cap \sum_{j \in J} X_j < X_i \,.$$

Then $E^+ = E \cup \{X\}$ *and* $E^- = E \setminus \{X\}$ *are in* $\Psi'(G,H) \setminus \Gamma(V,H)$ *. Moreover* $A_{E^+} = A_{E^-} = A_E = A$ *.*

Proof. $X < X_i$ implies that $A_{E^+} = A_{E^-} = A_E = A$. For the same reason, since $E \in \Psi'(G,H) \setminus \Gamma(V,H)$, we have that E^+, $E^- \notin \Gamma(V,H)$. Now we verify that E^- and E^+ are in $\Psi'(G,H)$. Clearly $E^- \in \Psi'(G,H)$ since $E^- \subseteq E$. As concerns E^+ , just notice that, if $g \in G$ stabilizes each $T \in E$, then g stabilizes each $X_i \in A = A_E$. So $g \in \mathrm{stab}_G(X)$. Indeed

$$(X_i \cap \sum_{j \in J} X_j)g = X_i g \cap \sum_{j \in J} X_j g = X_i \cap \sum_{j \in J} X_j \,.$$

□

Corollary 4.3.16. *Let* $A = \{X_1, \ldots, X_k\} \in \mathcal{A}$*. If there exists some* $i \in \{1, \ldots, k\}$ *and* $J \subseteq \{1, \ldots, k\}$ *such that*

$$0 < X := X_i \cap \sum_{j \in J} X_j < X_i \,,$$

then

$$\sum_{\substack{E \in \Psi'(G,H) \setminus \Gamma(V,H) \\ A_E = A}} (-1)^{|E|} = 0 \,.$$

Proof. By proposition 4.3.15, there is a bijection

$$\beta : \{E \mid A_E = A \,,\, E = E^+\} \to \{E \mid A_E = A \,,\, E = E^-\}$$

given by: $E \mapsto E^-$. The corollary follows from the remark that exactly one of E^+ , E^- is equal to E. Thus

$$(-1)^{|E^+|} + (-1)^{|E^-|} = 0 \,.$$

□

We give a direct proof of the following lemma for the lattice $\mathcal{S}(V,H)$ of H-invariant subspaces, although a similar result can be generalized to all finite modular lattices. We remind that, by Proposition 2.2.9, every finite modular lattice is graded, hence it admits a rank function.

Lemma 4.3.17. *Let V be a vector space of finite dimension over $\mathbb{F}_q$, and let $H \leq G = \mathrm{GL}(V)$. Let $A = \{X_1, \dots, X_k\}$ be an antichain in $\mathcal{S}(V,H)^*$ satisfying the following three conditions:*

(*a*) $\sum_{i=1}^{k} X_i = V$ *;*

(*b*) *there do not exist* $W_1, W_2 \in \mathcal{S}(V,H)$ *such that*

1) $V = W_1 \oplus W_2$ *and*
2) *each* X_i *is contained in either* W_1 *or* W_2 *;*

(*c*) $\forall\, i \in \{1,\dots,k\}$ *and* $\forall\, J \subseteq \{1,\dots,k\}$

$$X_i \cap \sum_{j\in J} X_j \in \{0, X_i\}\,.$$

Then all the X_i *have the same rank in* $\mathcal{S}(V,H)$*.*

Proof. Let $r = \mathrm{rk}(V)$ be the rank of V in $\mathcal{S}(V,H)$ and proceed by induction on r. If $r = 1$, the claim is trivially true. So, let $r > 1$ and $q_i = \mathrm{rk}(X_i) < r$ in $\mathcal{S}(V,H)$. We may assume that $k > 1$ and $q_1 \leq q_2 \leq \dots \leq q_k$. We first show that $q_{k-1} = q_k$. By conditions (*b*) and (*c*), we have that

$$X_k \leq \sum_{i=1}^{k-1} X_i\,.$$

By (*c*) we know that $X_k \cap X_1 = 0$ and there exists some $j \in \{2,\dots,k-1\}$ such that

$$X_k \leq \sum_{i=1}^{j} X_i \ \text{ and } \ X_k \cap \sum_{i=1}^{j-1} X_i = 0\,.$$

For this j, we have $X_j \nleq \sum_{i=1}^{j-1} X_i$, hence $X_j \cap \sum_{i=1}^{j-1} X_i = 0$. This implies that

$$q_k + \mathrm{rk}\left(\sum_{i=1}^{j-1} X_i\right) = \mathrm{rk}\left(X_k + \sum_{i=1}^{j-1} X_i\right) \leq \mathrm{rk}\left(X_k + \sum_{i=1}^{j} X_i\right)$$
$$\leq \mathrm{rk}\left(\sum_{i=1}^{j} X_i\right) = q_j + \mathrm{rk}\left(\sum_{i=1}^{j-1} X_i\right),$$

and therefore, $q_k = q_j = q_{k-1}$.
Now let $\overline{V} = V/X_k$, and let $\overline{T} = (T + X_k)/X_k$ for each $T \in \mathcal{S}(V,H)$.

Claim: $\{\overline{X_i}\}_{i\in\{1,\dots,k-1\}}$ is an antichain in $\mathcal{S}(\overline{V},H)$ satisfying conditions $(a),(b),(c)$ with respect to $\overline{V}$.

If it is true, then by inductive hypothesis all the $\overline{X_i}$ have the same rank in

$\mathcal{S}(\overline{V}, H)$. By (c), $\mathrm{rk}(\overline{X}_i)$ in $\mathcal{S}(\overline{V}, H)$ is equal to $q_i = \mathrm{rk}(X_i)$ in $\mathcal{S}(V, H)$.

Proof of the claim. We assume that $\overline{X}_i \cap \overline{X}_j \neq 0$ for some $i, j \in \{1, \ldots, k-1\}$. This means that

$$x_i + X_k = x_j + X_k$$

for some $x_i \in X_i$ and $x_j \in X_j$. Thus $x_i \in X_j + X_k$ and $x_j \in X_i + X_k$ and by condition (c) we have $X_i \subseteq X_j + X_k$ and $X_j \subseteq X_i + X_k$. Thus,

$$X_i + X_k = X_j + X_k$$

and $\overline{X}_i = \overline{X}_j$. Therefore $\{\overline{X}_i\}_{i \in \{1,\ldots,k-1\}}$ is an antichain. Clearly this antichain satisfies (a) with respect to $\overline{V}$.

Suppose that $\{\overline{X}_i\}_{i \in \{1,\ldots,k-1\}}$ does not satisfy (b) with respect to $\overline{V}$. Then there exist $\overline{W}_1, \overline{W}_2 \in\in \mathcal{S}(\overline{V}, H)$ such that $\overline{V} = \overline{W}_1 \oplus \overline{W}_2$ and each $\overline{X}_i$ is contained in either $\overline{W}_1$ or $\overline{W}_2$. Let W_1, W_2 be the respective preimages of $\overline{W}_1, \overline{W}_2$ in V. We define

$$I_1 = \{i \in \{1, \ldots, k-1\} \mid \overline{X}_i \leq \overline{W}_1\} \text{ and } I_2 = \{i \in \{1, \ldots, k-1\} \mid \overline{X}_i \leq \overline{W}_2\}.$$

Since the $\overline{X}_i$ satisfy (a) with respect to $\overline{V}$, we notice that

$$\{X_i \mid i \in I_1\} \cup \{X_k\}$$

is an antichain in $\mathcal{S}(W_1, H)$ satisfying (a) and (c) with respect to W_1. Similarly, $\{X_i \mid i \in I_2\} \cup \{X_k\}$ is an antichain in $\mathcal{S}(W_2, H)$ satisfying (a) and (c) with respect to W_2. By the definition of $\overline{W}_1, \overline{W}_2$, we have that $W_1 \cap W_2 = X_k$. If $\{X_i \mid i \in I_1\} \cup \{X_k\}$ does not satisfy (b) with respect to W_1, then there exist $Y_1, Y_2 \in \mathcal{S}(W_1, H)$ such that $W_1 = Y_1 \oplus Y_2$ and each of the $X_i \subseteq W_1$ is contained in either Y_1 or Y_2. We may assume that $X_k \subseteq Y_1$. But then, $V = (W_2 + Y_1) \oplus Y_2$ and each of the $X_i \in A$ is contained in either $W_2 + Y_1$ or Y_2, contradicting the fact that our original antichain satisfies (b) with respect to V. Therefore $\{X_i \mid i \in I_1\} \cup \{X_k\}$ must also satisfy condition (b) with respect to W_1 and these $X_i \subseteq W_1$ have the same rank in $\mathcal{S}(W_1, H)$ by inductive hypothesis. A similar argument may be applied to W_2. This means that $q_i = q_k$ for all $i \in \{1, \ldots, k\}$.

Finally, we verify (c) on $\overline{V}$. Let

$$\overline{X}_i \cap \sum_{j \in J} \overline{X}_j \neq 0$$

for some $i \in \{1, \ldots, k-1\}$ and $J \subseteq \{1, \ldots, k-1\}$. Then we must also have

$$X_i \cap (X_k + \sum_{j \in J} X_j) \neq 0$$

and, by condition (c) with respect to V, $X_i \leq X_k + \sum_{j \in J} X_j$. Therefore $\overline{X}_i \subseteq \sum_{j \in J} \overline{X}_j$ and $\{\overline{X}_i\}_{i \in \{1,\ldots,k-1\}}$ satisfies (c) with respect to $\overline{V}$. □

Lemma 4.3.17, together with Corollary 4.3.16, implies that

$$\sum_{E\in\Psi'(G,H)\setminus\Gamma(V,H)} (-1)^{|E|} = 0$$

if $\mathcal{S}(V,H)$ is a distributive lattice of prime rank. This is the first result in the following section §4.4. Then, we will try to say something about

$$\sum_{E\in\Psi'(G,H)\cap\Gamma(V,H)} (-1)^{|E|} .$$

4.4 Distributive lattices of H-invariant subspaces

In this section we will always assume that the lattice $\mathcal{S}(V,H)$ is distributive. We recall that such a lattice can be either boolean (e.g., take $H=\bigoplus_{i=1}^r \mathrm{GL}(W_i)$, with $V=\bigoplus_{i=1}^r W_i$) or non-boolean (e.g., take the stabiliser of a complete flag in dimension $n\geq 2$).

In general, by Proposition 4.2.4, we have that

$$-\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G) = \sum_{E\in\Psi'(G,H)} (-1)^{|E|}$$

where

$$\Psi'(G,H) = \{E\subseteq \mathcal{S}(V,H)^* \mid \bigcap_{W\in E} \mathrm{stab}_G(W)\neq H\} .$$

We can split the sum into

$$\sum_{E\in\Psi'(G,H)\cap\Gamma(V,H)} (-1)^{|E|} \; + \sum_{E\in\Psi'(G,H)\setminus\Gamma(V,H)} (-1)^{|E|} . \tag{4.15}$$

In the following theorem we assume that $\mathcal{S}(V,H)$ is a distributive lattice of prime rank.

Theorem 4.4.1. *Let V be a vector space of finite dimension over $\mathbb{F}_q$, and let $H\leq G\leq \mathrm{GL}(V)$. Let $\mathcal{S}(V,H)$ be distributive. Let $A=\{X_1,\dots,X_k\}$ be an antichain in $\mathcal{S}(V,H)^*$ such that $A\in\Psi'(G,H)\setminus\Gamma(V,H)$. If V has prime rank in $\mathcal{S}(V,H)$, then*

$$\sum_{\substack{E\in\Psi'(G,H)\setminus\Gamma(V,H)\\ A_E=A}} (-1)^{|E|} = 0 .$$

Proof. Suppose for contradiction that

$$\sum_{\substack{E\in\Psi'(G,H)\setminus\Gamma(V,H)\\ A_E=A}} (-1)^{|E|} \neq 0 .$$

Since $A \in \Psi'(G,H) \setminus \Gamma(V,H)$, by Corollary 4.3.16 we have that A satisfies conditions $(a),(b),(c)$ of Lemma 4.3.17. Let $J \subseteq \{1,\ldots,k\}$ be minimal with respect to the property that $\sum_{j\in J} X_j = V$. Then, by condition (c), $V = \bigoplus_{j\in J} X_j$. Since $\mathrm{rk}(V)$ is prime and all the X_i have the same rank in $\mathcal{S}(V,H)$, we have that $\mathrm{rk}(X_i) = 1\ \forall i$. Then each $X_i \in A$ is an atom, and therefore join-irreducible, in $\mathcal{S}(V,H)$. Since $\mathcal{S}(V,H)$ is distributive, by Lemma 2.2.13 we have that if $X_i \in A$ then $X_i \leq X_j$ for some $j \in J$. Then it is possible to write $V = W_1 \oplus W_2$ so that each X_i is contained in either W_1 or W_2. But this contradicts condition (b) of lemma 4.3.17. □

Then, the second term in (4.15) vanishes under the same assumptions.

Corollary 4.4.2. *Let V be a linear space of finite dimension over $\mathbb{F}_q$, and let $H \leq G = \mathrm{GL}(V)$. Let $\mathcal{S}(V,H)$ be distributive. If V has prime rank in $\mathcal{S}(V,H)$, then*

$$-\,\mu_{\mathcal{I}_1(G,H)}(H,G) = \sum_{E\in\Psi'(G,H)\cap\Gamma(V,H)} (-1)^{|E|}\,. \tag{4.16}$$

What can we say about (4.16)?

By using the definition of $\Psi'(G,H)$, that is,

$$\Psi'(G,H) = \{E \subseteq \mathcal{S}(V,H)^* \mid \bigcap_{W\in E} \mathrm{stab}_G(W) \neq H\}\,, \tag{4.17}$$

we immediately have the following general proposition (not only for distributive lattices).

Proposition 4.4.3. *Let V be a linear space of finite dimension over $\mathbb{F}_q$, and let $H \leq G = \mathrm{GL}(V)$. If for every $E \in \Gamma(V,H)$ there exists an element $g \in G$ such that*

$$g \in \bigcap_{W\in E} \mathrm{stab}_G(W) \quad \textit{but} \quad g \notin H, \tag{4.18}$$

then $\Gamma(V,H) \subseteq \Psi'(G,H)$. In particular,

$$\sum_{E\in\Psi'(G,H)\cap\Gamma(V,H)} (-1)^{|E|} = \sum_{E\in\Gamma(V,H)} (-1)^{|E|}\,. \tag{4.19}$$

Example 4.4.4. By Proposition 4.5.11 in §4.5, we will see an example in which the condition (4.18) is satisfied.

So, by Corollary 4.4.2, if $\mathcal{S}(V,H)$ is distributive of prime rank, then one could be interested in computing

$$\sum_{E\in\Gamma(V,H)} (-1)^{|E|} \tag{4.20}$$

to obtain $\mu_{\mathcal{I}_1(G,H)}(H,G)$, provided that the condition (4.18) in Proposition 4.4.3 holds true.

In §4.4.1 and §4.4.2 we compute (4.20), showing that it is 0 by the following theorem.

Theorem 4.4.5. *Let V be a vector space of finite dimension over $\mathbb{F}_q$. Let H be a reducible subgroup of $\mathrm{GL}(V)$. If the lattice $\mathcal{S}(V,H)$ of H-invariant subspaces is distributive, then*

$$\sum_{E \in \Gamma(V,H)} (-1)^{|E|} = 0$$

Remark. Actually, the same proof shows more generally that, if $X \in \mathcal{S}(V,H)$ satisfies

- $\mathrm{rk}(X) \geq 2$ in $\mathcal{S}(V,H)$ and the sublattice $\mathcal{S}(X,H)$ is distributive,

then

$$\sum_{E \in \Gamma(X,H)} (-1)^{|E|} = 0.$$

By proposition 4.3.3, we know that

$$\sum_{E \in N(V,H)} (-1)^{|E|} = -\mu_{\mathcal{S}(V,H)}(0,V)\,.$$

The proof is divided into two cases.

- §4.4.1: $\mathcal{S}(V,H)$ is boolean;
- §4.4.2: $\mathcal{S}(V,H)$ is distributive, but non-boolean.

We recall that $\Gamma(V,H) = N(V,H) \sqcup D(V,H)$, hence

$$\sum_{E \in \Gamma(V,H)} (-1)^{|E|} = \sum_{E \in N(V,H)} (-1)^{|E|} + \sum_{E \in D(V,H)} (-1)^{|E|}\,. \tag{4.21}$$

In both cases, we will compute separately the two terms on the right-hand side of (4.21).

4.4.1 The boolean case

Let $\mathcal{S}(V,H)$ be boolean. First of all, by Theorem 4.3.2, independently of the structure of $\mathcal{S}(V,H)$ we have that

$$\sum_{E \in N(V,H)} (-1)^{|E|} = -\mu_{\mathcal{S}(V,H)}(0,V).$$

Therefore, by Theorem 3.1.14, we immediately obtain that

$$\sum_{E \in N(V,H)} (-1)^{|E|} = (-1)^{r+1} \tag{4.22}$$

where $r = |\mathrm{JI}(\mathcal{S}(V,H))|$ is the number of join-irreducible elements of $\mathcal{S}(V,H)$. We recall that in a boolean lattice every join-irreducible element is an atom. In particular, $\mathcal{S}(V,H)$ is isomorphic to a direct product of r chains of length 1 and V is the direct sum of all atoms of $\mathcal{S}(V,H)$.

The proof of Theorem 4.4.5 for a boolean $\mathcal{S}(V,H)$ relies in the two following lemmas. Before we state the first lemma, we remark an application of Proposition 4.3.11.

Remark. If $\mathcal{S}(V,H)$ is boolean and $\mathrm{JI}(\mathcal{S}(V,H)) = \{P_1,\dots,P_r\}$ is the set of its atoms, then we have a proper direct decomposition of rank 1 given by

$$\Delta_1 = \{P_1,\dots,P_r\}. \tag{4.23}$$

By Proposition 4.3.11, we observe that $\Delta_1 = \{P_1,\dots,P_r\}$ is the unique proper direct decomposition of rank 1 for $\mathcal{S}(V,H)$. This fact is useful in the proof of Theorem 4.4.5 for the boolean case.

Lemma 4.4.6. *Let* $\mathrm{JI}(\mathcal{S}(V,H)) = \{P_1,\dots,P_r\}$ *be the set of atoms in* $\mathcal{S}(V,H)$*. Let* $\Delta_1 = \Delta_1(V,H) \in \mathfrak{D}(V,H)$ *be the unique proper direct decomposition of rank* 1 *in* $\mathfrak{D}(V,H)$*, so that* $\Delta_1 = \{P_1,\dots,P_r\}$*. Then*

$$\sum_{\substack{E \in D(V,H) \\ \partial(E) = \Delta_1(V,H)}} (-1)^{|E|} = (-1)^r \,.$$

Proof. It is clear that the unique $E \in D(V,H)$ such that $\partial(E) = \Delta_1(V,H)$ must be

$$E = \{P_1,\dots,P_r\}\,.$$

Therefore,

$$\sum_{\substack{E \in D(V,H) \\ \partial(E) = \Delta_1(V,H)}} (-1)^{|E|} = (-1)^r \,.$$

□

Remark. Let $\mathrm{JI}(\mathcal{S}(V,H)) = \{P_1,\dots,P_r\}$ is the set of atoms in the boolean lattice $\mathcal{S}(V,H)$. Let Δ be a direct decomposition of V in $\mathcal{S}(V,H)$, so that $\Delta = \{S_1,\dots,S_l\}$. If $\mathrm{rk}_{\mathfrak{D}}(\Delta) = m \geq 2$ (i.e. $\Delta \neq \Delta_1(V,H)$ of Lemma 4.4.6), then

$$\exists\, i \in \{1,\dots,l\} \text{ such that } \quad S_i = P_{j_1} + \cdots + P_{j_m}\,.$$

Lemma 4.4.7. *Let* $\mathrm{JI}(\mathcal{S}(V,H)) = \{P_1, \dots, P_r\}$ *be the set of atoms in* $\mathcal{S}(V,H)$*. Let* $\Delta = \{S_1, \dots, S_l\} \in \mathfrak{D}(V,H)$ *be a proper direct decomposition such that* $\mathrm{rk}_{\mathfrak{D}}(\Delta) \geq 2$*. Then*

$$\sum_{\substack{E \in D(V,H) \\ \partial(E)=\Delta}} (-1)^{|E|} = 0\,.$$

Proof. We proceed by induction on the rank of Δ. If $\mathrm{rk}_{\mathfrak{D}}(\Delta) = 2$, then there exists S_i of rank 2, namely $S_i = P_{j_1} + P_{j_2}$. Let $E \in D(V,H)$ such that $\partial(E) = \Delta$. This implies that $S_i \in E$, since P_{j_1} and P_{j_2} are atoms in direct sum. Now assume that $P_{j_1} \in E$. Then we have another $E^- \in D(V,H)$, given by $E \setminus P_{j_1}$, such that $\Delta(E^-) = \Delta$. Notice that

$$(-1)^{|E|} + (-1)^{|E^-|} = 0\,.$$

And conversely, for each $E \in D(V,H)$ such that $\partial(E) = \Delta$ and $P_{j_1} \notin E$, we have $E^+ = E \cup \{P_{j_1}\}$. So, in general, for any Δ of rank 2, there is a 1-to-1 correspondence between

$$\left\{ \begin{array}{c} E^+ \in D(V,H) \ \text{s.t.} \\ \partial(E^+) = \Delta \text{ and } P_{j_1} \in E \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} E^- \in D(V,H) \ \text{s.t.} \\ \partial(E^-) = \Delta \text{ and } P_{j_1} \notin E^- \end{array} \right\}.$$

Thus

$$\sum_{\substack{E \in D(V,H) \\ \partial(E)=\Delta}} (-1)^{|E|} = 0\,.$$

Now let $M \in \mathbb{N}$, $M > 2$, and assume that the result holds for each $\delta \in \mathfrak{D}(V,H)$ of rank m, with $2 \leq m \leq M-1$. We prove that it holds true also for Δ of rank M. Let $\Delta = \{S_1, \dots, S_l\}$. By Corollary 4.3.8, we have that

$$\sum_{\substack{E \in D(V,H) \\ \partial(E)=\Delta}} (-1)^{|E|} = (-1)^l \prod_{j=1}^{l} \sum_{F \in \Gamma(S_j,H)} (-1)^{|F|}\,.$$

There exists S_i of rank M in $\mathcal{S}(V,H)$, i.e.

$$S_i = P_{j_1} + \cdots + P_{j_M}$$

for some atoms $P_{j_1}, \dots, P_{j_M}$ in $\mathcal{S}(V,H)$. By proposition 2.3.7, the sublattice

$$\mathcal{S}(S_i,H) = \{T \in \mathcal{S}(V,H) \mid T \leq S_i\}$$

is boolean. Its atoms are $P_{j_1}, \dots, P_{j_M}$. Clearly, if we prove that

$$\sum_{F \in \Gamma(S_i,H)} (-1)^{|F|} = 0\,,$$

we are done. So we write

$$\sum_{F\in\Gamma(S_i,H)}(-1)^{|F|}=\sum_{F\in N(S_i,H)}(-1)^{|F|}+\sum_{F\in D(S_i,H)}(-1)^{|F|}\,.$$

By proposition 4.3.3 and theorem 3.1.14, we have that

$$\sum_{F\in N(S_i,H)}(-1)^{|F|}=-\mu_{\mathcal{S}(S_i,H)}(0,S_i)=(-1)^{M+1}\,.$$

Moreover, by the same argument that we have seen for $D(V,H)$, we obtain that

$$\sum_{F\in D(S_i,H)}(-1)^{|F|}=\sum_{\substack{E\in D(S_i,H)\\ \partial(E)=\Delta_1(S_i,H)}}(-1)^{|E|}+\sum_{\substack{\Delta\in\mathfrak{D}(S_i,H)\\ \Delta\neq\Delta_1(S_i,H)}}\left(\sum_{\substack{E\in D(S_i,H)\\ \partial(E)=\Delta}}(-1)^{|E|}\right)$$

$$=(-1)^M+\sum_{\substack{\Delta\in\mathfrak{D}(S_i,H)\\ \Delta\neq\Delta_1(S_i,H)}}\left(\sum_{\substack{E\in D(S_i,H)\\ \partial(E)=\Delta}}(-1)^{|E|}\right)\,.$$

Let $\delta\in\mathfrak{D}(S_i,H)$. Then the rank of δ is $<M$. Let $P_{j_{M+1}},\dots,P_{j_r}$ be all the remaining $r-M$ atoms in $\mathcal{S}(V,H)$ such that

$$S_i\cap P_{j_{M+1}}=\cdots=S_i\cap P_{j_r}=0\,.$$

We define

$$\Delta'=\delta\cup\{P_{j_{M+1}},\dots,P_{j_r}\}$$

and observe that $\Delta'\in\mathfrak{D}(V,H)$. Moreover, we have that $2\leq rk_{\mathfrak{D}}(\Delta')<M$. Then, by inductive hypothesis

$$\sum_{\substack{E\in D(V,H)\\ \partial(E)=\Delta'}}(-1)^{|E|}=0\,.$$

Since $P_{j_{M+1}},\dots,P_{j_r}$ are atoms in $\mathcal{S}(V,H)$, we have that

$$\sum_{\substack{E\in D(V,H)\\ \partial(E)=\Delta'}}(-1)^{|E|}=\sum_{\substack{E\in D(S_i,H)\\ \partial(E)=\delta}}(-1)^{|E|+r-M}=(-1)^{r-M}\sum_{\substack{E\in D(S_i,H)\\ \partial(E)=\delta}}(-1)^{|E|}.$$

Thus

$$0=(-1)^{r-M}\sum_{\substack{E\in D(S_i,H)\\ \partial(E)=\delta}}(-1)^{|E|}\quad\Rightarrow\quad 0=\sum_{\substack{E\in D(S_i,H)\\ \partial(E)=\delta}}(-1)^{|E|}$$

and finally

$$\sum_{F\in\Gamma(S_i,H)} (-1)^{|F|} = (-1)^{M+1} + (-1)^{M} = 0\,.$$

□

Lemma 4.4.6 and Lemma 4.4.7 prove the following.

Proposition 4.4.8. *Let V be a linear space of finite dimension over $\mathbb{F}_q$, and let $H \leq \mathrm{GL}(V)$. If $\mathcal{S}(V,H)$ is boolean, then*

$$\sum_{E\in D(V,H)} (-1)^{|E|} = (-1)^{r} \tag{4.24}$$

where $r = |\mathrm{JI}(\mathcal{S}(V,H))|$ is the number of join-irreducible elements in $\mathcal{S}(V,H)$.

Therefore, by putting together (4.22) and (4.24), we have proven Theorem 4.4.5 when $\mathcal{S}(V,H)$ is boolean.

4.4.2 The non-boolean case

If $\mathcal{S}(V,H)$ is a distributive lattice, but it is not boolean, then

$$\sum_{E\in N(V,H)} (-1)^{|E|} = -\mu_{\mathcal{S}(V,H)}(0,V) = 0 \tag{4.25}$$

by Theorem 4.3.2 and Theorem 3.1.14.

In this case, in order to prove Theorem 4.4.5 it suffices that

$$\sum_{E\in D(V,H)} (-1)^{|E|} = 0\,.$$

As in the boolean case, we first need a lemma.

Lemma 4.4.9. *Let V be a vector space of finite dimension over $\mathbb{F}_q$, and $H \leq \mathrm{GL}(V)$. Let $\mathcal{S}(V,H)$ be a non-boolean distributive lattice.*

- *(i) There exists a subspace $W \in \mathcal{S}(V,H)$ such that $W \neq 0$ and W is covered by a join-irreducible element of $\mathcal{S}(V,H)$.*
- *(ii) Let $W \in \mathcal{S}(V,H)$, $W \neq 0$, and assume that W is covered by a join-irreducible element of $\mathcal{S}(V,H)$. If $E \in D(V,H)$, we define $E^+ = E \cup \{W\}$ and $E^- = E \setminus \{W\}$. Then E^+ and E^- are in $D(V,H)$.*

Proof.
(i). Since $\mathcal{S}(V,H)$ is distributive, but it is not boolean, by Corollary 2.2.17 there exists a join-irreducible element Q in $S_V(H)$ that is not an atom, i.e. Q is join-irreducible and it covers a subspace $W \in \mathcal{S}(V,H)$, with $W \neq 0$.

(ii). Let $E = \{V_1, \dots, V_t\} \in D(V,H)$ such that

$$\sum_{k=1}^{t} V_k = V = \bigoplus_{j=1}^{r} S_j \,,$$

where $\{S_1, \dots, S_r\} \in \mathfrak{D}(V,H)$ and for each k there exists j such that $V_k \subseteq S_j$. As above, let Q be a join-irreducible subspace covering W in $\mathcal{S}(V,H)$. So we have

$$W < Q \leq \sum_{i=1}^{u} V_{k_i}$$

with $V_{k_1}, \dots, V_{k_u} \in E$, $u \in \{1, \dots, t\}$. Notice that E^+ and E^- are distinct collections of non-trivial subspaces in $\mathcal{S}(V,H)$, since E^+ contains W and E^- does not. Moreover, $E = E^+$ or $E = E^-$. First we show that both E^+ and E^- generate V. If $E = E^-$, then clearly also $E \cup \{W\}$ spans V. On the other hand, assume that $E = E^+$, so that $W = V_s$ for some $s \in \{1, \dots, t\}$. By Lemma 2.2.13, since Q is join-irreducible,

$$Q \leq \sum_{i=1}^{u} V_{k_i} \quad \Rightarrow \quad Q \leq V_{k_i} \text{ for some } i \in \{1, \dots, u\}.$$

So we have

$$W = V_s < Q \leq V_{k_i} \quad \Rightarrow \quad W = V_s < V_{k_i} \quad \Rightarrow \quad \sum_{\substack{1 \leq k \leq t \\ k \neq s}} V_k = V \,,$$

which means that also $E \setminus \{W\}$ generates V. In general, by the previous argument based on Lemma 2.2.13, we have shown that $W < V_k$ for some $k \in \{1, \dots, t\}$, with $V_k \neq W$. Now it is easy to see that the direct decomposition $\{S_1, \dots, S_r\}$, which we have defined for $E \in D(V,H)$, is suitable for both E^+ and E^-. Therefore, we conclude that both E^+ and E^- are in $D(V,H)$. □

By applying the above Lemma 4.4.9, we directly obtain the following proposition. Together with (4.25), it gives Theorem 4.4.5 when $\mathcal{S}(V,H)$ is distributive and non-boolean.

Proposition 4.4.10. *Let V be a vector space of finite dimension over $\mathbb{F}_q$, and $H \leq \mathrm{GL}(V)$. Let $\mathcal{S}(V,H)$ be a non-boolean distributive lattice. Then*

$$\sum_{E \in D(V,H)} (-1)^{|E|} = 0 \,. \tag{4.26}$$

Proof. Assume that $D(V,H) \neq \emptyset$, otherwise there is nothing to show. So, by (i) of Lemma 4.4.9 we know that there exists a subspace $W \in \mathcal{S}(V,H)$

such that $W \neq 0$ and W is covered by a join-irreducible element of $\mathcal{S}(V,H)$. Then there is a 1-to-1 correspondence between

$$\left\{ \ E^+ \in D(V,H) \ \text{ s.t. } W \in E^+ \ \right\} \longleftrightarrow \left\{ \ E^- \in D(V,H) \ \text{ s.t. } W \notin E^- \ \right\}$$

given by (ii) of Lemma 4.4.9.
Notice that clearly

$$(-1)^{|E^+|} + (-1)^{|E^-|} = 0\,.$$

Thus

$$\sum_{E \in D(V,H)} (-1)^{|E|} = 0\ .$$

□

4.5 An example in $\mathrm{GL}(n,q)$

In general, the lattice $\mathcal{S}(V,H)$ is not distributive. In this section we present an example of a family of subgroups H in $\mathrm{GL}(V)$, for $V = \mathbb{F}_q^n$, so that the structure of the correspondent $\mathcal{S}(V,H)$ is not distributive, except for some special cases that we consider preliminarily. The aim is to show that the same methods studied in the previous sections of this chapter can be reworked for different classes of subgroups.

We start with fixing the notation, defining our family of subgroups $H \leq \mathrm{GL}(V)$, and showing the special cases which could be known by Shareshian's results contained in [38] or by what we have previously presented. Then we will concentrate on the other subgroups of the family and we will see some general properties related to their reducible subgroup ideal $\mathcal{I}_1(G,H)$. In particular, we will obtain again that

$$\sum_{E \in \Psi'(G,H) \setminus \Gamma(V,H)} (-1)^{|E|} = 0$$

if the rank $\mathrm{rk}(V)$ of V in $\mathcal{S}(V,H)$ is prime.

Notation and special cases

Let $V \simeq \mathbb{F}_q^n$ be a vector space of finite dimension over $\mathbb{F}_q$. Let r be a positive integer such that $0 \leq r \leq n$. If $r \geq 1$, for $i = 1,\dots,r$ let $m_i \in \mathbb{N}$ so that

$$m_1 + \cdots + m_r \leq n.$$

Then we fix the following basis of V:

$$\mathcal{E} = \{w_1^{(1)},\dots,w_{m_1}^{(1)},\dots,w_1^{(r)},\dots,w_{m_r}^{(r)},v_1,\dots,v_{n-(m_1+\cdots+m_r)}\}$$

so that

$$V = \langle w_1^{(1)}, \ldots, w_{m_1}^{(1)} \rangle \oplus \cdots \oplus \langle w_1^{(r)}, \ldots, w_{m_r}^{(r)} \rangle \oplus \langle v_1, \ldots, v_{n-(m_1+\cdots+m_r)} \rangle .$$

So, we have that

$$V = W_1 \oplus \cdots \oplus W_r \oplus W^c$$

where

$$\begin{aligned} W_1 &:= \langle w_1^{(1)}, \ldots, w_{m_1}^{(1)} \rangle \simeq V(m_1, q) \\ &\vdots \\ W_r &:= \langle w_1^{(r)}, \ldots, w_{m_r}^{(r)} \simeq V(m_r, q) \rangle \end{aligned}$$

and

$$W^c := \langle v_1, \ldots, v_{n-(m_1+\cdots+m_r)} \rangle \simeq V(n - (m_1 + \cdots + m_r), q) .$$

represents the canonical complement of $W_1 \oplus \cdots \oplus W_r$ in V with respect to base $\mathcal{E}$. We denote by W the sum

$$W = W_1 \oplus \cdots \oplus W_r$$

so that $V = W \oplus W^c$.

Let $G = \mathrm{GL}(V) \simeq \mathrm{GL}(n, q)$. Similarly we have $\mathrm{GL}(W_i) \simeq \mathrm{GL}(m_i, q)$. Moreover we call Z_{W^c} the centre of the group $\mathrm{GL}(W^c)$, that is the subgroup

$$Z_{W^c} = Z(\mathrm{GL}(W^c)) = \{ z I_{W^c} \mid z \in \mathbb{F}_q^* \}$$

consisting of the scalar transformations. We denote Z_{W^c} also as Z_d, if d is the dimension of W^c.

We consider the following class of subgroups $H \leq G$:

$$H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Z_{W^c} \tag{4.27}$$

such that

$$H \simeq \mathrm{GL}(m_1, q) \oplus \cdots \oplus \mathrm{GL}(m_r, q) \oplus Z_{n-(m_1+\cdots+m_r)} \tag{4.28}$$

with $0 \leq r \leq n$ and $m_1 + \cdots + m_r \leq n$.

We observe that we also include the following special cases:

- $r = 0$, meaning that $H = Z_n$;
- $m_1 + \cdots + m_r = n$, meaning that $H = \mathrm{GL}(m_1, q) \oplus \cdots \oplus \mathrm{GL}(m_r, q)$.

We see that H is an intersection of maximal subgroups of $G = \mathrm{GL}(V)$, as follows. We recall that the stabilizers of subspaces in $\mathrm{GL}(V)$ are maximal subgroups of $\mathrm{GL}(V)$ (this is part of Aschbacher's classification, but for a direct proof one can also see [22]). So, for any $0 < U < V$ the subgroup $\mathrm{stab}_G(U)$ is maximal in G. Let

$$K = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus \mathrm{GL}(W^c).$$

Then

$$K = \mathrm{stab}_G(W_1) \cap \cdots \cap \mathrm{stab}_G(W_r) \cap \mathrm{stab}_G(W^c) \tag{4.29}$$

is an intersection of maximal subgroups of $\mathrm{GL}(V)$. Now, if $m_1 + \cdots + m_r = n$, we have that $\dim(W^c) = 0$ and consequently $H = K$. Then, by (4.29), H is an intersection of maximal subgroups of $\mathrm{GL}(V)$. Otherwise, we know that W^c is not the only complement of W in the subspace lattice of V. Let

$$\mathcal{W}^{\perp} = \{T \leq V \mid V = W \oplus T\}$$

be the set of all complements of W in $\mathcal{S}_V$. Then

$$\bigcap_{T \in \mathcal{W}^{\perp}} \mathrm{stab}_G(T) = \mathrm{GL}(W) \oplus Z_{W^c} \tag{4.30}$$

is an intersection of maximal subgroup of G. Therefore,

$$H = K \cap \bigcap_{T \in \mathcal{W}^{\perp}} \mathrm{stab}_G(T) \tag{4.31}$$

is an intersection of maximal subgroups of G.

What is $\mathcal{S}(V, H)$ for such a subgroup H? We can observe that if $r = 0$, i.e. $H = Z_n$, then $\mathcal{S}(V, H) = \mathcal{S}(V, Z_n) = \mathcal{S}_V$ is the subspace lattice of V. On the opposite, if $W^c = 0$ and we have that $H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r)$ for $V = \bigoplus_{i=1}^r W_i$, then the lattice $\mathcal{S}(V, H)$ is boolean, since the only H-invariant subspaces are the sums of the $W_1, \ldots, W_r$. In particular, $W_1, \ldots, W_r$ are the atoms of $\mathcal{S}(V, H)$. In general, by elementary linear algebra, we can state the following proposition that characterizes the H-invariant subspaces.

Proposition 4.5.1. *Let $V \simeq \mathbb{F}_q^n$, so that $V = W_1 \oplus \cdots \oplus W_r \oplus W^c$. Let*

$$H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Z_{W^c} \leq \mathrm{GL}(V).$$

Then, the H-invariant subspaces of V are of the form:

(a) $T \leq W^c$;

(b) $T + W_{i_1} + \cdots + W_{i_k}$, with $1 \leq i_1 < i_2 < \cdots < i_k \leq r$ and $T \leq W^c$.

The following definition is related to Proposition 4.5.1 and it will be used throughout this chapter.

Definition 4.5.2. Let $V \simeq \mathbb{F}_q^n$, so that $V = W_1 \oplus \cdots \oplus W_r \oplus W^c$. Let

$$H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Z_{W^c} \leq \mathrm{GL}(V)\,.$$

We say that a subspace $S \leq V$ is **mixed** if

$$S = \sum_{i \in I} W_i + T$$

where $\emptyset \neq I \subseteq \{1, \ldots, r\}$ and $0 < T \leq W^c$.

By Proposition 4.5.1, every mixed subspace is H-invariant. Since $\mathcal{S}(V, H)$ is a modular lattice, by Theorem 2.2.9 it is also graded.

Remark. Let $\mathrm{rk} : \mathcal{S}(V, H) \to \mathbb{N}$ denote the rank function of $\mathcal{S}(V, H)$, for H as above. Let $W = W_1 \oplus \cdots \oplus W_r$. Let $m_i = \dim(W_i)$ and $m = m_1 + \cdots + m_r$. In particular we observe that

- $\mathrm{rk}(W_i) = 1$ for all $i = 1, \ldots, r$;
- $\mathrm{rk}(W) = r$;
- $\mathrm{rk}(W^c) = \dim(V/W) = n - m$;
- $\mathrm{rk}(V) = n - m + r$.

Special cases

In this section we briefly review some special cases of the example that we are considering. More precisely, we have the following extreme cases.

(*a*) $r = 0$ and $H = Z_n$. This case has been considered by Shareshian in [38].

(*b*) $n - m = \dim(W^c) = 0$ and $r \geq 1 \Rightarrow H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r)$. In this case, the lattice $\mathcal{S}(V, H)$ is boolean. It is isomorphic to the product of r chains of length 1.
Similarly, if $n - m = \dim(W^c) = 1$ and $r \geq 1$ we have that $H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Z_{W^c}$, where $Z_{W^c} \simeq \mathbb{F}_q^*$. Also in this case, the lattice $\mathcal{S}(V, H)$ is boolean.

We consider now these cases separately, just to highlight some relevant facts.

Shareshian's results for $r = 0$

This is the case described by Shareshian to find $\mu(1, \mathrm{PGL}(n,q))$. Actually, he obtains some partial results using the arguments that we have generalized in Chapter 4. Since

$$\mu(1, \mathrm{PGL}(n,q)) = \mu(Z_n, \mathrm{GL}(n,q))$$

we can consider $H = Z_n \leq \mathrm{GL}(n,q) = G$. Shareshian observes that

$$\Gamma(V,H) \subseteq \Psi'(G,H)$$

and, if the dimension n is prime, then

$$\mu_{\widehat{\mathcal{I}}_1(G,H)} = \sum_{E \in \Gamma(V,H)} (-1)^{|E|} = \frac{|\mathrm{GL}(V)|}{n(q^n - 1)} .$$

If n is small, we have not only that many of the geometrical classes $\mathcal{C}_i(G,H)$, for $i = 1, \ldots, 8$, are empty, but also that the class $\mathcal{C}_9(G,H)$ may be known. Here, as an example, we list some results for $\mathrm{PGL}(n,q)$.

Theorem 4.5.3 ([38], Theorem 1.7 and Theorem 1.8)**.**
If $p > 3$ is prime and if $n = 2$, then

$$\mu(1, \mathrm{PGL}(2, p^a)) = \rho(a) \cdot |\mathrm{PSL}(2, p^a)|$$

where

$$\rho(a) = \begin{cases} 1 & \text{if } a = 1,\ p \equiv 3, 5 \bmod 8\,; \\ 0 & \text{otherwise.} \end{cases}$$

If $p = 3$, then

$$\mu(1, \mathrm{PGL}(2, 3^a)) = \sigma(a) \cdot |\mathrm{PSL}(2, 3^a)|$$

where

$$\sigma(a) = \begin{cases} -\mu(a) & \text{if } a \text{ is odd;} \\ 0 & \text{if } a \text{ is even.} \end{cases}$$

Theorem 4.5.4 ([38], Theorem 1.9)**.** *Let $V \simeq \mathbb{F}_q^3$, with $q = p^a$ for an odd prime p. If $\mathrm{PSL}(V) < \mathrm{PGL}(V)$, then $\mu(1, \mathrm{PGL}(V)) = 0$.*

By using the same argument, he similarly obtains also a result for PSL(3, q).

Theorem 4.5.5 ([38], Theorem 1.9)**.** *Let p be an odd prime and let a be a positive integer. Then*

$$\mu(1, \mathrm{PSL}(3, p^a)) = \begin{cases} -6|\mathrm{PSL}(3, p^a)| & \text{if } a = 1 \text{ and } p \equiv 1, 4 \bmod 15; \\ -6|\mathrm{PSL}(3, p^a)| & \text{if } a = 2 \text{ and } p \equiv 2, 7, 8, 13 \bmod 15; \\ 0 & \text{otherwise.} \end{cases}$$

Boolean lattices

Boolean lattice can arise from $\mathcal{S}(V,H)$, for some cases in the family of subgroups H that we are considering.

For instance, if $n-(m_1+\cdots+m_r)=0$ and $r=1$, then $H=\mathrm{GL}(V)=G$ and $\mathcal{S}(V,H)=\{0,V\}$. Here we know that, by definition, $\mu(G,H)=\mu(G,G)=1$.

Now, let $n-(m_1+\cdots+m_r)=0$ and $r\geq 1$. Then

$$H=\mathrm{GL}(W_1)\oplus\cdots\oplus\mathrm{GL}(W_r).$$

In this case we could be interested in

$$\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G)=-\sum_{E\in\Psi'(G,H)}(-1)^{|E|}.$$

Even though we know by Theorem 4.4.5 that

$$\sum_{E\in\Gamma(V,H)}(-1)^{|E|}=0,$$

we have that in general

$$\sum_{E\in\Psi'(G,H)}(-1)^{|E|}\neq 0\,.$$

An example is the following.

Example 4.5.6. Let $r=2$. Then $\mathcal{S}(V,H)^*=\{W_1,W_2\}$, and we have that $D(V,H)=\{\{W_1,W_2\}\}$ is not contained in $\Psi'(G,H)$. On the opposite, here we have $N(V,H)=\{\emptyset,\{W_1\},\{W_2\}\}=\Psi'(G,H)$ and

$$\sum_{E\in\Psi'(G,H)}(-1)^{|E|}=-1\,.$$

Remark. We observe that if $n-(m_1+\cdots+m_r)=1$ and $r\geq 1$. Then

$$H=\mathrm{GL}(W_1)\oplus\cdots\oplus\mathrm{GL}(W_r)\oplus Z_{W^c}$$

where $Z_{W^c}\simeq\mathrm{GL}(W^c)\simeq\mathbb{F}_q^*$. So, we can write H as

$$H=\mathrm{GL}(W_1)\oplus\cdots\oplus\mathrm{GL}(W_r)\oplus\mathrm{GL}(W^c)$$

and the lattice $\mathcal{S}(V,H)$ is boolean with $r+1$ atoms.

We want to state the following Proposition 4.5.7, because it will be used in §4.5 as an inductive step in the proof of Proposition 4.5.16.

Proposition 4.5.7. *Let $V = W \oplus T$ be a vector space of finite dimension n over $\mathbb{F}_q$, so that $W = W_1 \oplus \cdots \oplus W_r$ and $\dim(T) = 1$. Let $H \leq \mathrm{GL}(V)$ such that*

$$H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus \mathrm{GL}(T)\,.$$

Let

$$X = \sum_{i \in I} W_i + T$$

be a mixed subspace of V, for some $I \subseteq \{1, \ldots, r\}$, $\emptyset \neq I$. Then

$$\sum_{E \in \Gamma(X,H)} (-1)^{|E|} = 0\,.$$

Proof. If $\dim(T) = 1$, there is no non-trivial H-invariant subspace of W^c. By Proposition 2.3.7, the lattice $\mathcal{S}(X,H)$ is boolean, since $\mathcal{S}(V,H)$ is boolean. Then, by Proposition 4.4.5,

$$\sum_{E \in \Gamma(X,H)} (-1)^{|E|} = 0\,.$$

□

Now we can introduce a general method, that is strictly related to Shareshian's argument and what we have seen in §4.4. It may be useful if one is interested in computing

$$\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G).$$

The case with $r \geq 1$ and $n - m \geq 2$

We present now a more general argument that can be used with the following conditions for n, m, r:

$$r \geq 1 \quad \text{and} \quad n - m \geq 2$$

where $m = m_1 + \cdots + m_r$. This assumption will remain valid in all results presented in this section, unless otherwise stated.

Actually in this case, for the group H that we are considering, we are able to prove only Theorem 4.5.8 and Corollary 4.5.9, obtaining that

$$\sum_{E \in \Psi'(G,H) \setminus \Gamma(V,H)} (-1)^{|E|} = 0$$

if $\mathrm{rk}(V)$ in $\mathcal{S}(V,H)$ is prime. Unfortunately, we can not use our methods to compute

$$\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G)$$

because it is impossible to apply the criterion of Proposition 4.4.3, as we will explain in Example 4.5.10. For this reason, we will define another subgroup

$$H_1 = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Id_{W^c}$$

such that

- $\mathcal{S}(V,H) = \mathcal{S}(V,H_1)$, and
- we can apply to H_1 the criterion of Proposition 4.4.3.

For H_1, we will prove that

$$\mu_{\widehat{\mathcal{I}}_1(G,H_1)}(H_1,G) = 0$$

if the rank of V in $\mathcal{S}(V,H_1)$ is prime.

Now we prove that

$$\sum_{E\in\Psi'(G,H)\setminus\Gamma(V,H)} (-1)^{|E|} = 0$$

if $\mathrm{rk}(V)$ in $\mathcal{S}(V,H)$ is prime. The proof of this fact is very similar to the proof that we have seen in Theorem 4.4.1.

Theorem 4.5.8. *Let $V = W \oplus W^c$ be a vector space of finite dimension n over $\mathbb{F}_q$, so that $W = W_1 \oplus \cdots \oplus W_r$. Let $H \leq \mathrm{GL}(V)$ such that*

$$H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Z_{W^c}\,.$$

Let $A = \{X_1, \ldots, X_k\}$ be an antichain in $\mathcal{S}(V,H)^*$ such that $A \in \Psi'(G,H)\setminus \Gamma(V,H)$. If the rank of V in $\mathcal{S}(V,H)$ is prime, then

$$\sum_{\substack{E\in\Psi'(G,H)\setminus\Gamma(V,H)\\ A_E=A}} (-1)^{|E|} = 0\,.$$

Proof. Suppose for contradiction that

$$\sum_{\substack{E\in\Psi'(G,H)\setminus\Gamma(V,H)\\ A_E=A}} (-1)^{|E|} \neq 0\,.$$

By corollary 4.3.16 and since $A \in \Psi'(G,H)\setminus\Gamma(V,H)$, we have that A satisfies conditions $(a),(b),(c)$ of lemma 4.3.17. Let $J \subseteq \{1,\ldots,k\}$ be minimal with respect to the property that $\sum_{j\in J} X_j = V$. Then, by condition (c), $V = \bigoplus_{j\in J} X_j$. Since $\mathrm{rk}(V)$ is prime and all the X_i have the same rank in $\mathcal{S}(V,H)$, we have that $\mathrm{rk}(X_i) = 1\ \forall i$. Then either $X_i \in \{W_1,\ldots,W_r\}$ or $X_i = T$, where T is some subspace of W^c of dimension 1 in V. So each X_i is contained either in W or in W^c. Then we have contradiction with (b) of lemma 4.3.17. □

As an immediate consequence we obtain the following corollary.

Corollary 4.5.9. *Let $V = W \oplus W^c$ be a vector space of finite dimension n over $\mathbb{F}_q$, so that $W = W_1 \oplus \cdots \oplus W_r$. Let $H \leq \mathrm{GL}(V)$ such that*

$$H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Z_{W^c}\,.$$

Let the rank of V be prime in $\mathcal{S}(V, H)$. Then

$$\sum_{E \in \Psi'(G,H) \setminus \Gamma(V,H)} (-1)^{|E|} = 0$$

and

$$-\mu_{\mathcal{I}_1(G,H)}(H, G) = \sum_{E \in \Psi'(G,H) \cap \Gamma(V,H)} (-1)^{|E|}\,.$$

In the following section, we give a general criterion that can be used to reduce the calculation of

$$-\mu_{\mathcal{I}_1(G,H)}(H, G) = \sum_{E \in \Psi'(G,H) \cap \Gamma(V,H)} (-1)^{|E|}$$

to the calculation of

$$\sum_{E \in \Gamma(V,H)} (-1)^{|E|}.$$

Application of the criterion of Proposition 4.4.3

By Corollary 4.5.9, we want to compute

$$-\mu_{\mathcal{I}_1(G,H)}(H, G) = \sum_{E \in \Psi'(G,H) \cap \Gamma(V,H)} (-1)^{|E|}$$

in order to find $\mu_{\mathcal{I}_1(G,H)}(H, G)$. The calculation could be easier if we had $\Gamma(V, H) \subseteq \Psi'(G, H)$, because in this case we would have that

$$\sum_{E \in \Psi'(G,H) \cap \Gamma(V,H)} (-1)^{|E|} = \sum_{E \in \Gamma(V,H)} (-1)^{|E|}$$

In particular, we recall that

$$\Psi'(G, H) = \{E \subseteq \mathcal{S}(V, H)^* \mid \bigcap_{W \in E} \mathrm{stab}_G(W) \neq H\}\,.$$

As we have shown in Proposition 4.4.3, $\Gamma(V, H) \subseteq \Psi'(G, H)$ if for every $E \in N(V, H) \sqcup D(V, H)$ there exists an element $g \in G$ such that

$$g \in \bigcap_{W \in E} \mathrm{stab}_G(W) \quad \text{but} \quad g \notin H \tag{4.32}$$

where $G = \mathrm{GL}(V)$ is acting in a natural way on the subspace lattice $\mathcal{S}_V$.

Remark. In [38], the subgroup considered by Shareshian is the centre of $\mathrm{GL}(V)$, i.e. $H = Z_V = Z(G)$, and we have that $\Gamma(V, Z_V) \subseteq \Psi'(G, Z_V)$. Indeed, if $E \in N(V, Z_V)$ or $E \in D(V, Z_V)$, then there exist two subspaces $U, W \leq V$ such that $V = U \oplus W$. So, we can define $g \in \mathrm{GL}(V)$ such that $g_{|U} = I_U$ and $g_{|W} = -I_W$. Then, this element g satisfies (4.32), because $g \notin Z_V$.

Finding such an element in G for all $E \in \Gamma(V, H)$ is not an easy task at all. Sometimes it is even impossible, as shown in the following example.

Example 4.5.10. Let $V = W_1 \oplus \cdots \oplus W_r \oplus W^c$ and $H \leq \mathrm{GL}(V)$ such that

$$H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Z_{W^c}.$$

Consider the following element E of $D(V, H)$ given by the collection

$$E = \{W_1, \ldots, W_r, \text{ all subspaces of } W^c\}.$$

$E \in D(V, H)$ since $W_1 \oplus \cdots \oplus W_r \oplus W^c$ is a non-trivial direct decomposition of V. There follows that

$$H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Z_{W^c} = \bigcap_{T \in E} \mathrm{stab}_G(T),$$

hence an element g as in (4.32) does not exist.

So, unfortunately, it is not possible to use this criterion directly with the subgroup H. Now, we consider a modified version of H given by the subgroup

$$H_1 = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Id_{W^c},$$

such that the criterion can be applied with the following element

$$g = \begin{bmatrix} I_m & 0 \\ 0 & -I_{n-m} \end{bmatrix} = \begin{bmatrix} Id_W & 0 \\ 0 & -Id_{W^c} \end{bmatrix} \in G \quad \& \quad g \notin H_1$$

where $\dim(W) = m$ and $\dim(W^c) = n - m$.

For H_1, we can state the following proposition.

Proposition 4.5.11. *Let $V = W \oplus W^c$ be a vector space of finite dimension n over $\mathbb{F}_q$, so that $W = W_1 \oplus \cdots \oplus W_r$. Let $G = \mathrm{GL}(V)$ and $H_1 \leq G$ such that*

$$H_1 = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Id_{W^c}.$$

Then $\Gamma(V, H_1) \subseteq \Psi'(G, H_1)$.

We decide to investigate the sum

$$\sum_{E\in\Gamma(V,H_1)} (-1)^{|E|}$$

for H_1, since by Proposition 4.5.11 and Corollary 4.5.9 we have that

$$-\mu_{\widehat{\mathcal{I}}_1(G,H_1)}(H_1,G) = \sum_{E\in\Psi'(G,H_1)} (-1)^{|E|} = \sum_{E\in\Gamma(V,H_1)} (-1)^{|E|}\,.$$

Indeed, $\Gamma(V,H_1) \subseteq \Psi'(G,H_1)$ and

$$\sum_{E\in\Psi'(G,H)\setminus\Gamma(V,H_1)} (-1)^{|E|} = 0.$$

We also notice that $\mathcal{S}(V,H_1) = \mathcal{S}(V,H)$. So, we can write

$$-\mu_{\widehat{\mathcal{I}}_1(G,H_1)}(H_1,G) = \sum_{E\in\Gamma(V,H)} (-1)^{|E|}\,. \tag{4.33}$$

We remark that

$$\sum_{E\in\Gamma(V,H)} (-1)^{|E|} = \sum_{E\in N(V,H)} (-1)^{|E|} + \sum_{E\in D(V,H)} (-1)^{|E|} \tag{4.34}$$

and we proceed by computing separately

$$\sum_{E\in N(V,H)} (-1)^{|E|} \quad \text{and} \quad \sum_{E\in D(V,H)} (-1)^{|E|}\,.$$

The sum over the non-spanning sets

Notation. As previously noted, $\mathcal{S}(V,H_1) = \mathcal{S}(V,H)$. Then, we also have that $N(V,H) = N(V,H_1)$, $D(V,H) = D(V,H_1)$, $\Gamma(V,H) = \Gamma(V,H_1)$. Since the following results are related only to the subspace lattice (which is the same for H and H_1), we only use the terms with H to simplify the notation. All the obtained results can be similarly referred to H_1.

Now we compute

$$\sum_{E\in N(V,H)} (-1)^{|E|} = \sum_{E\in N(V,H_1)} (-1)^{|E|}\,.$$

By Proposition 4.3.3 we have that

$$\sum_{E\in N(V,H)} (-1)^{|E|} = -\mu_{\mathcal{S}(V,H)}(0,V)\,.$$

Remind that $V = W \oplus W^c$, where $W = W_1 \oplus \cdots \oplus W_r$, and that we know the H-invariants subspaces in $\mathcal{S}(V,H)$ (Proposition 4.5.1). We use this to compute $\mu_{\mathcal{S}(V,H)}(0,V)$. Firstly, we prove a lemma.

Lemma 4.5.12. *Let $V = W \oplus W^c$ be a vector space of finite dimension n over $\mathbb{F}_q$, so that $W = W_1 \oplus \cdots \oplus W_r$. Let $H \leq \mathrm{GL}(V)$ be such that*

$$H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Z_{W^c}.$$

Then for any $1 \leq i_1 < i_2 < \cdots < i_k \leq r$ and for any $T \leq W^c$, we have

$$\sum_{0 \leq S \leq T} \mu_{\mathcal{S}(V,H)}(0, S + W_{i_1} + \cdots + W_{i_k}) = 0.$$

In particular

$$\sum_{0 \leq T \leq W^c} \mu_{\mathcal{S}(V,H)}(0, T + W_{i_1} + \cdots + W_{i_k}) = 0.$$

Proof. Let $T \leq W^c$ be any subspace. The proof is by induction on k. Let $k = 1$. If we consider $T + W_{i_1} \in \mathcal{S}(V,H)$, with $W_{i_1} \in \{W_1, \ldots, W_r\}$, then

$$\begin{aligned} \mu_{\mathcal{S}(V,H)}(0, T + W_{i_1}) &= - \sum_{\substack{0 \leq S < T + W_{i_1} \\ S \in \mathcal{S}(V,H)}} \mu_{\mathcal{S}(V,H)}(0, S) \\ &= - \sum_{0 \leq S \leq T} \mu_{\mathcal{S}(V,H)}(0, S) - \sum_{0 \leq S < T} \mu_{\mathcal{S}(V,H)}(0, S + W_{i_1}) \end{aligned}$$

and

$$\sum_{0 \leq S \leq T} \mu_{\mathcal{S}(V,H)}(0, S) = 0$$

by definition of the Möbius function. This implies that

$$\sum_{0 \leq S \leq T} \mu_{\mathcal{S}(V,H)}(0, S + W_{i_1}) = 0$$

for each $T \leq W^c$. Assume now that for any $1 \leq j_1 < j_2 < \cdots < j_u \leq r$, with $u < k$, we have

$$\sum_{0 \leq S \leq T} \mu_{\mathcal{S}(V,H)}(0, S + W_{j_1} + \cdots + W_{j_u}) = 0.$$

Let $1 \leq i_1 < i_2 < \cdots < i_k \leq r$ and $X := T + W_{i_1} + \cdots + W_{i_k}$. Then

$$\mu_{\mathcal{S}(V,H)}(0, X) = - \sum_{\substack{0 \leq S < X \\ S \in \mathcal{S}(V,H)}} \mu_{\mathcal{S}(V,H)}(0, S).$$

By Proposition 4.5.1 we can classify the subspaces of X in $\mathcal{S}(V,H)$ in the following families

$\mathcal{F}_1 := \{Y \mid Y \leq T\};$

$\mathcal{F}_2 := \{Y + W_{j_1} + \cdots + W_{j_u} \mid Y \leq T,\ \{j_1, \ldots, j_u\} \subset \{i_1, \ldots, i_k\} \text{ with } u < k\};$

$\mathcal{F}_3 := \{Y + W_{i_1} + \cdots + W_{i_k} \mid Y < T\}.$

So

$$\mu_{\mathcal{S}(V,H)}(0, X) = -\sum_{S \in \mathcal{F}_1} \mu_{\mathcal{S}(V,H)}(0, S) - \sum_{S \in \mathcal{F}_2} \mu_{\mathcal{S}(V,H)}(0, S) - \sum_{S \in \mathcal{F}_3} \mu_{\mathcal{S}(V,H)}(0, S)\,.$$

But

$$\sum_{S \in \mathcal{F}_1} \mu_{\mathcal{S}(V,H)}(0, S) = \sum_{0 \leq S \leq T} \mu_{\mathcal{S}(V,H)}(0, S) = 0.$$

Moreover, by inductive hypothesis, also

$$\sum_{S \in \mathcal{F}_2} \mu_{\mathcal{S}(V,H)}(0, S) = 0\,.$$

Finally we obtain

$$\mu_{\mathcal{S}(V,H)}(0, X) = -\sum_{S \in \mathcal{F}_3} \mu_{\mathcal{S}(V,H)}(0, S) = -\sum_{0 \leq Y < T} \mu_{\mathcal{S}(V,H)}(0, Y + W_{i_1} + \cdots + W_{i_k})$$

whence

$$\sum_{0 \leq S \leq T} \mu_{\mathcal{S}(V,H)}(0, S + W_{i_1} + \cdots + W_{i_k}) = 0\,.$$

□

Now we can prove the following Proposition 4.5.13 and compute $\mu_{\mathcal{S}(V,H)}(0, V)$, in order to get

$$\sum_{E \in N(V,H)} (-1)^{|E|}\,.$$

Proposition 4.5.13. *Let $V = W \oplus W^c$ be a vector space of finite dimension n over $\mathbb{F}_q$, so that $W = W_1 \oplus \cdots \oplus W_r$. Let $H \leq \mathrm{GL}(V)$ be such that*

$$H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Z_{W^c}\,.$$

Let X be a mixed subspace of V,

$$X = \sum_{i \in I} W_i + T$$

where $\emptyset \neq I \subseteq \{1, \ldots, r\}$ and $0 < T \leq W^c$. Then

$$\begin{aligned}\sum_{E \in N(X,H)} (-1)^{|E|} &= -\mu_{\mathcal{S}(X,H)}(0, X)\\ &= (-1)^{|I|+1} \mu_{\mathcal{S}(T,H)}(0, T)\\ &= (-1)^{|I|+1} (-1)^{\dim(T)}\, q^{\binom{\dim(T)}{2}}\,.\end{aligned}$$

Proof. By lemma 4.5.12 we have that

$$\sum_{0\le S\le T} \mu_{\mathcal{S}(V,H)}(0, S+W) = 0$$

for any $T \le W^c$. Notice that

$$\mu_{\mathcal{S}(V,H)}(0,V) = \mu_{\mathcal{S}(V,H)}(0, W^c + W_1 + \cdots + W_r).$$

So, in particular,

$$\sum_{0\le T\le W^c} \mu_{\mathcal{S}(V,H)}(0, T + W_1 + \cdots + W_r) = 0\,.$$

Therefore

$$\mu_{\mathcal{S}(V,H)}(0,V) = -\sum_{0\le T< W^c} \mu_{\mathcal{S}(V,H)}(0, T + W_1 + \cdots + W_r)\,.$$

Now we observe that

$$\mu_{\mathcal{S}(V,H)}(0, W_1 + W_2 + \cdots + W_r) = \mu_{\mathcal{S}(W,H)}(0, W_1 + W_2 + \cdots + W_r)$$

and, since the lattice $\mathcal{S}_W(H)$ is boolean, by theorem 3.1.14

$$\mu_{\mathcal{S}(V,H)}(0, W_1 + W_2 + \cdots + W_r) = (-1)^r\,.$$

Thus we can sum up the above information in the following conditions:

$$\begin{cases} \sum_{0\le S\le T} \mu_{\mathcal{S}(V,H)}(0, S+W) = 0 & \text{if } 0 \ne T \le W^c, \\ \mu_{\mathcal{S}(V,H)}(0, W) = (-1)^r\,. \end{cases}$$

Then

$$\mu_{\mathcal{S}(V,H)}(0,V) = (-1)^r \mu_{\mathcal{S}_{W^c}}(0, W^c)$$

where $\mu_{\mathcal{S}_{W^c}}$ is the Möbius function on the lattice of subspaces of W^c. By Proposition 4.3.2 we obtain

$$\mu_{\mathcal{S}(V,H)}(0,V) = (-1)^r (-1)^{n-(m_1+\cdots+m_r)}\, q^{\binom{n-(m_1+\cdots+m_r)}{2}}\,.$$

□

Corollary 4.5.14. *Let $V = W \oplus W^c$ be a vector space of finite dimension n over $\mathbb{F}_q$, so that $W = W_1 \oplus \cdots \oplus W_r$. Let $H \le \mathrm{GL}(V)$ such that*

$$H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Z_{W^c}\,.$$

Let m_i be the dimension of each W_i, and let $m = m_1 + \cdots + m_r$. Then

$$\begin{aligned} \sum_{E\in N(V,H)} (-1)^{|E|} &= -\mu_{\mathcal{S}(V,H)}(0,V) \\ &= (-1)^{r+1} \mu_{\mathcal{S}_{W^c}}(0, W^c) \\ &= (-1)^{r+1} (-1)^{n-(m_1+\cdots+m_r)}\, q^{\binom{n-(m_1+\cdots+m_r)}{2}}\,. \end{aligned}$$

The sum over the decomposing sets and $\Gamma(V, H)$

Our final goal is to show that

$$\sum_{E \in \Gamma(V,H)} (-1)^{|E|} = 0\,,$$

or equivalently that

$$\sum_{E \in D(V,H)} (-1)^{|E|} = - \sum_{E \in N(V,H)} (-1)^{|E|}\,.$$

Let $V = W \oplus W^c$ be a vector space of finite dimension n over $\mathbb{F}_q$, so that $W = W_1 \oplus \cdots \oplus W_r$. Let $H \leq \mathrm{GL}(V)$ such that

$$H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Z_{W^c}\,.$$

Let $X \in \mathcal{S}(V, H) \setminus \{0\}$. We define

- $\mathfrak{D}(X, H)_0 \subseteq \mathfrak{D}(X, H)$ such that

$$\mathfrak{D}(X, H)_0 = \{\Delta \in \mathfrak{D}(X, H) \mid \exists \text{ mixed subspace } S \in \Delta\}\,.$$

- $\mathfrak{D}(X, H)^* = \mathfrak{D}(X, H) \setminus \mathfrak{D}(X, H)_0$.

Remark. Let $X \in \mathcal{S}(V, H) \setminus \{0\}$. By Proposition 4.3.6, if $E \subseteq \mathcal{S}(X, H)^*$ is such that $E \in D(X, H)$, then there exists a mixed subspace $S \in E$ if and only if $\partial(E) \in \mathfrak{D}(X, H)_0$.

Also in this case, we prove a preliminary lemma.

Lemma 4.5.15. *Let $V = W \oplus W^c$ be a vector space of finite dimension n over $\mathbb{F}_q$, so that $W = W_1 \oplus \cdots \oplus W_r$. Let $H \leq \mathrm{GL}(V)$ be such that*

$$H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Z_{W^c}\,.$$

Let $X \in \mathcal{S}(V, H) \setminus \{0\}$. Then

$$\sum_{\Delta \in \mathfrak{D}(X,H)^*} \left(\sum_{\substack{E \in D(X,H) \\ \partial(E) = \Delta}} (-1)^{|E|} \right) = - \sum_{E \in N(X,H)} (-1)^{|E|}\,.$$

Proof. Let $E \in D(V, H)$ be such that $\partial(E) \in \mathfrak{D}(V, H)^*$. This means that no mixed subspace is contained in $\partial(E)$, and consequently E does not contain any mixed subspace. We can write

$$E = F_1 \cup F_2, \qquad \text{with } F_1 \cap F_2 = \emptyset\,,$$

where F_1 is the set of subspaces in E contained in $W = W_1 \oplus \cdots \oplus W_r$; on the other hand, F_2 is the set of subspaces in E contained in W^c

- $F_1 = \{S \leq W \mid S \in E\}$;
- $F_2 = \{S \leq W^c \mid S \in E\}$.

Moreover E falls in one, and only one, of the following three cases:

(a) $E \setminus \{W\}$ is spanning for V, i.e. $\sum_{S \in E} S = V$ (and $E \setminus \{W\} \in D(V, H)$). It means also that $F_1 \setminus \{W\}$ is spanning for W.

(b) $E \setminus \{W\}$ is non-spanning for V, but $E \setminus \{W^c\}$ is spanning for V. In particular it implies that $F_1 \setminus \{W\}$ is non-spanning for W, so $W \in F_1$, but $F_2 \setminus \{W^c\}$ is spanning for W^c.

(c) $E \setminus \{W\}$ is non-spanning for V and $E \setminus \{W^c\}$ is non-spanning for V. This necessarily implies that $W, W^c \in E$. So both $F_1 \setminus \{W\}$ is non-spanning for W and $F_2 \setminus \{W^c\}$ is non-spanning for W^c.

In case (a), both $E'_a = E \setminus \{W\}$ and $E''_a = E \cup \{W\}$ are in $D(V, H)$, and $\partial(E'_a)$, $\partial(E''_a) \in \mathfrak{D}(V, H)^*$. Obviously $E \in \{E'_a, E''_a\}$, but most importantly

$$(-1)^{|E \setminus \{W\}|} + (-1)^{|E \cup \{W\}|} = 0\,.$$

This implies that the sum over all the addends $(-1)^{|E|}$, with E as in case (a), is 0.
In case (b), both $E'_b = E \setminus \{W^c\}$ and $E''_b = E \cup \{W^c\}$ are in $D(V, H)$, and $\partial(E'_b)$, $\partial(E''_b) \in \mathfrak{D}(V, H)^*$. Again $E \in \{E'_b, E''_b\}$, and we have

$$(-1)^{|E \setminus \{W^c\}|} + (-1)^{|E \cup \{W^c\}|} = 0\,.$$

This implies that the sum over all the addends $(-1)^{|E|}$, with E as in case (b), is 0.
So, for the sum

$$\sum_{\Delta \in \mathfrak{D}(V,H)^*} \left(\sum_{\substack{E \in D(V,H) \\ \partial(E) = \Delta}} (-1)^{|E|} \right)$$

we can just consider E as in case (c), where we have

$$E = F_1 \cup F_2 = F'_1 \cup F'_2 \cup \{W, W^c\}$$

so that $F'_1 = F_1 \setminus \{W\}$, $F'_2 = F_2 \setminus \{W^c\}$, and

$$F'_1 \in N(W, H)\,, \quad F'_2 \in N(W^c, H)\,.$$

Thus we can compute

$$\sum_{\Delta\in\mathfrak{D}(V,H)^*}\left(\sum_{\substack{E\in D(V,H)\\ \partial(E)=\Delta}}(-1)^{|E|}\right) = \sum_{F_1'\in N(W,H)}\left(\sum_{F_2'\in N(W^c,H)}(-1)^{|F_1'|+|F_2'|+2}\right)$$

$$= \sum_{F_1'\in N(W,H)}(-1)^{|F_1'|}\left(\sum_{F_2'\in N(W^c,H)}(-1)^{|F_2'|}\right).$$

By Proposition 4.5.13

$$\sum_{\Delta\in\mathfrak{D}(V,H)^*}\left(\sum_{\substack{E\in D(V,H)\\ \partial(E)=\Delta}}(-1)^{|E|}\right) = -\mu_{\mathcal{S}_{W^c}(H)}(0,W^c)\sum_{F_1'\in N(W,H)}(-1)^{|F_1'|}$$

$$= -\mu_{\mathcal{S}_{W^c}(H)}(0,W^c)\cdot(-\mu_{\mathcal{S}_{W}(H)}(0,W))$$

$$= -\mu_{\mathcal{S}_{W^c}(H)}(0,W^c)\cdot(-1)^{r+1}$$

$$= (-1)^r\,\mu_{\mathcal{S}_{W^c}(H)}(0,W^c)$$

$$= -\sum_{E\in N(V,H)}(-1)^{|E|}.$$

□

In particular, for $X = V$, we have that

$$\sum_{\Delta\in\mathfrak{D}(V,H)^*}\left(\sum_{\substack{E\in D(V,H)\\ \partial(E)=\Delta}}(-1)^{|E|}\right) = -\sum_{E\in N(V,H)}(-1)^{|E|}.$$

We use the previous result to conclude the main result about the sum

$$\sum_{E\in\Gamma(X,H)}(-1)^{|E|} = 0$$

for our subgroup H.

Theorem 4.5.16. *Let $V = W\oplus W^c$ be a vector space of finite dimension n over $\mathbb{F}_q$, so that $W = W_1\oplus\cdots\oplus W_r$. Let $H\leq \mathrm{GL}(V)$ be such that*

$$H = \mathrm{GL}(W_1)\oplus\cdots\oplus\mathrm{GL}(W_r)\oplus Z_{W^c}.$$

Let

$$X = \sum_{i \in I} W_i + T$$

be a mixed subspace of V*, for some* $I \subseteq \{1, \dots, r\}$*,* $\emptyset \neq I$*, and* $0 < T \leq W^c$*. Then*

$$\sum_{E \in \Gamma(X,H)} (-1)^{|E|} = 0\,. \tag{4.35}$$

In particular, if $X = V$*, we have that*

$$\sum_{E \in \Gamma(V,H)} (-1)^{|E|} = 0\,.$$

Proof. We proceed by induction on the rank of X. Since X is a mixed subspace in $\mathcal{S}(V,H)$, we observe that the minimal case is $\mathrm{rk}(X) = 2$, where X is necessarily of the form

$$X = W_i + T$$

for some $i \in \{1, \dots, r\}$ and $T \leq W^c$ such that $\dim(T) = 1$.
So, if $\mathrm{rk}(X) = 2$, then (4.35) is true by Proposition 4.5.7.
Now let $\mathrm{rk}(X) = k > 2$ and assume that (4.35) is true for every mixed subspace $Y \in \mathcal{S}(V,H)$ such that $\mathrm{rk}(Y) < k$. We want to prove that

$$\sum_{E \in \Gamma(X,H)} (-1)^{|E|} = 0\,.$$

We have

$$\begin{aligned} \sum_{E \in \Gamma(X,H)} (-1)^{|E|} &= \sum_{E \in N(X,H)} (-1)^{|E|} + \sum_{E \in D(X,H)} (-1)^{|E|} \\ &= \sum_{E \in N(X,H)} (-1)^{|E|} + \sum_{\Delta \in \mathfrak{D}(X,H)} \left(\sum_{\substack{E \in D(X,H) \\ \partial(E) = \Delta}} (-1)^{|E|} \right). \end{aligned}$$

But by Lemma 4.5.15, we know that

$$\sum_{\Delta \in \mathfrak{D}(X,H)^*} \left(\sum_{\substack{E \in D(X,H) \\ \partial(E) = \Delta}} (-1)^{|E|} \right) = - \sum_{E \in N(X,H)} (-1)^{|E|}\,.$$

Therefore

$$\sum_{E \in \Gamma(X,H)} (-1)^{|E|} = \sum_{\Delta \in \mathfrak{D}(X,H)_0} \left(\sum_{\substack{E \in D(X,H) \\ \partial(E) = \Delta}} (-1)^{|E|} \right)$$

and it suffices to prove that

$$\sum_{\Delta \in \mathfrak{D}(X,H)_0} \left(\sum_{\substack{E \in D(X,H) \\ \partial(E)=\Delta}} (-1)^{|E|} \right) = 0.$$

Let $\Delta \in \mathfrak{D}(X, H)_0$. Then Δ has rank $t < k$, i.e.

$$t = \max\{\mathrm{rk}(S) \mid S \in \Delta\} < k,$$

since the rank of X is k and Δ is a proper decomposition. So, Δ contains a mixed subspace $\widetilde{S}$ such that $\mathrm{rk}(\widetilde{S}) < k$. By inductive hypothesis

$$\sum_{E \in \Gamma(\widetilde{S},H)} (-1)^{|E|} = 0\,.$$

Then

$$\sum_{\substack{E \in D(X,H) \\ \partial(E)=\Delta}} (-1)^{|E|} = 0$$

by Lemma 4.3.7, and therefore we obtain (4.35) for X. □

Remark. We have seen that

$$\sum_{E \in \Gamma(V,H)} (-1)^{|E|} = \sum_{E \in \Gamma(V,H_1)} (-1)^{|E|} = 0\,.$$

Therefore

$$\mu_{\mathcal{I}_1(G,H_1)}(H_1, G) = 0 \tag{4.36}$$

where

$$H_1 = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Id_{W^c}\,.$$

In Chapter 5, we will define a closure operator on the subgroup lattice of G and we will obtain again this result as a particular case of the fact that every non-closed subgroup K in G has $\mu_{\mathcal{I}_1(G,K)}(K, G) = 0$ (see Proposition 5.2.3). In the situation we have presented above, H_1 is non-closed with respect to such a closure operator. On the contrary,

$$H = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r) \oplus Z_{W^c}$$

is closed, and H is precisely the closure of H_1 in the subgroup lattice $\mathcal{L}(G)$.

Some very particular case

Following the idea suggested by Shareshian in [38], we recall that one could write $\mu(H,G)$ through a function $f_{G,n,p}(u,H)$ so that

$$\mu(H, G(n,\, p^u)) = f_{G,n,p}(u,H) + \sum_{K\in\mathcal{C}_9} \mu(H,K)\,, \tag{4.37}$$

where $f_{G,n,p}(u,H)$ depends on the classes $\mathcal{C}_i(G,H)$, for $i = 1,\ldots,8$, in Aschbacher's classification. We could try to find the contribution given to the function $f_{G,n,p}$ by these classes, wondering when they are empty, so that their contribution is equal to 0. Combining this kind of results with our knowledge of $\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G)$, we could obtain the exact value of $\mu(H,G)$. This is clearly not easy in general.

In a very particular situation, related to the example that we have seen in this section, we get the following result.

Theorem 4.5.17. *Let $G = \mathrm{GL}(n,q)$, and let $H \le G$ be such that*

$$H = \mathrm{GL}(m,q) \oplus I_{n-m}\,.$$

Let $q = p$ be an odd prime and let the dimension n be prime. If $n-m+1$ is prime, then

$$f_{G,n,p}(H) = 0$$

and in particular

$$\mu(H,G) = \sum_{K\in\mathcal{C}_9(G,H)\,,\, H\subseteq K} \mu_K(H)\,.$$

Proof. By Theorem 4.5.16 and by using the condition that the rank of V in $\mathcal{S}(V,H)$ is $n-m+1$ and it is prime, we get that

$$-\mu_{\widehat{\mathcal{I}}_1(G,H_1)}(H_1,G) = \sum_{E\in\Psi'(G,H_1)} (-1)^{|E|} = \sum_{E\in\Gamma(V,H_1)} (-1)^{|E|} = 0.$$

By [21, Table 3.5.A], we see that H is not contained in any maximal subgroup of the classes $\mathcal{C}_i$ for $i = 2,\ldots,8$. This is essentially because of the prime dimension n and the prime order q of the field. □

In general, we do not have much information about the ninth class. Just to give an example, we considered the groups of low dimension studied by Schröder in his PhD thesis ([37]), and we saw that in dimension $n = 13$ also class $\mathcal{C}_9(G,H)$ is empty for $p > 5$. In this case, $\mu(H,G) = 0$.

Chapter 5

Reducible subgroups and a closure operator

In [10] Colombo and Lucchini solve Conjecture 3.2.10 for the family of all symmetric and alternating groups, i.e. $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$, with $n \geq 5$. One of the key ingredients in their argument is Crapo's Closure Theorem (Theorem 3.1.9), that is applied to the lattice of subgroups $\mathcal{L}(G)$, for $G \in \{\mathrm{Sym}(n), \mathrm{Alt}(n)\}$. In §5.1.1 of this chapter, we briefly remind Colombo-Lucchini's argument and then we show how it is possible to define a closure operator also for the subgroup lattice of a finite irreducible subgroup G of $\mathrm{GL}(n, q)$. In this way, we can express $\mu_G(H)$ as

$$\mu_G(H) = \sum_{K \in Irr_G(H)} \mu(K, G) \cdot g(H, K)$$

where $Irr_G(H)$ denotes the set of irreducible subgroups of G containing H. The function g comes from Crapo's Closure Theorem. In section §5.2, we revisit this argument by substituting the function g with the Möbius number of the ideal $\mathcal{I}_1(K, H)$ for any irreducible subgroup K of G. This is possible by Theorem 3.1.13 that we have shown in Chapter 3. We prove that

$$\mu_{\mathcal{I}_1(K,H)}(H, K) = g(H, K) = 0$$

if H is not a closed subgroup in K, similarly to what happens in Colombo-Lucchini's argument. Therefore, if $\mu_G(H) \neq 0$, then there exists at least one subgroup $K \in Irr_G(H)$ such that $\mu_G(K) \neq 0$ and H is closed in K. By using Proposition 5.3.2, we explain why it may be interesting to count the number of closed subgroups in $G = \mathrm{GL}(n, q)$ in order to estimate the number of subgroups $H \leq G = \mathrm{GL}(n, q)$ such that $\mu_G(H) \neq 0$. Our related results are contained in §5.3, where we assume that H is a subgroup of $G = \mathrm{GL}(n, q)$ such that the lattice $\mathcal{S}(V, H)$ is isomorphic to a product of chains.

5.1 Closure operators on subgroup lattices

In this section we recall the notion of a closure operator, and we see the example used for the symmetric group by Colombo and Lucchini in [10]. They prove that if G is a finite transitive permutation group, then in order to bound the number of subgroups $H \leq G$ with $\mu_G(H) \neq 0$ and to estimate $|\mu_G(H)|$, it suffices to obtain

(I) similar bounds for the particular case when H is transitive;

(II) estimations on the number of subgroups of G that are maximal with respect to the property of admitting a certain set of orbits.

In case G is an irreducible finite linear group, we can define a similar closure operator by using the join-irreducible subspaces of $\mathcal{S}(V, H)$, for $H \leq G$. This definition is given in §5.1.2.

5.1.1 Transitive permutation groups

Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group on a finite set Ω. A **closure operator** (in the sense of Definition 3.1.8) considered by Colombo and Lucchini in [10] is

$$^{-}\colon \mathcal{L}(G) \to \mathcal{L}(G)$$

such that for all $H \leq G$ we have the closure

$$\overline{H} := (\mathrm{Sym}(\Lambda_1) \times \cdots \times \mathrm{Sym}(\Lambda_k)) \cap G\,,$$

where $\{\Lambda_1, \ldots, \Lambda_k\}$ is the set of orbits of H with respect to its action on Ω. Clearly, we have identified H with a subgroup of $(\mathrm{Sym}(\Lambda_1)\times\cdots\times\mathrm{Sym}(\Lambda_k)) \leq \mathrm{Sym}(\Omega)$.

We say that H is a **closed subgroup** of G if $\overline{H} = H$.

Notation. We have that

$$\overline{\mathcal{L}(G)} = \{H \in \mathcal{L}(G) \mid \overline{H} = H\}$$

is the subposet of closed subgroups in $\mathcal{L}(G)$. Since G is transitive, $G \in \overline{\mathcal{L}(G)}$. Moreover, for any $H \in \overline{\mathcal{L}(G)}$ we write

$$\mu_{\overline{\mathcal{L}(G)}}(H, G)$$

to denote the Möbius function associated with $\overline{\mathcal{L}(G)}$.

Remark. It is worth noticing that in general $\overline{\mathcal{L}(H)} \neq \overline{\mathcal{L}(G)} \cap \mathcal{L}(H)$ when H is a transitive permutation subgroup of G on Ω.

Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group on a finite set Ω, and Let $H \leq G$. Then we define:

- the subset

$$\mathcal{T}(H) = \{K \leq G \mid H \leq K \text{ and } K \text{ is transitive on } \Omega\} \subseteq \mathcal{L}(G)$$

of all transitive subgroups of G containing H;

- the function $g : \mathcal{L}(G) \times \mathcal{L}(G) \to \mathbb{Z}$ such that

$$g(H,Y) = \begin{cases} \mu_{\overline{\mathcal{L}(Y)}}(H,Y) & \text{if } Y \in \mathcal{T}(H) \text{ and } H \in \overline{\mathcal{L}(Y)} \\ 0 & \text{otherwise.} \end{cases}$$

The following proposition allows us to write $\mu_G(H)$, for all $H \leq G$, in terms of $\mu_G(K)$ and $g(H,K)$, where K ranges over all transitive subgroups of G. Such an expression is useful in [10] to give estimates for Conjecture 3.2.10. In the proof, there is also an interesting use of Crapo's Closure Theorem (Theorem 3.1.9), together with Möbius Inversion Formula (Theorem 3.1.11).

Proposition 5.1.1 ([10], Lemma 1.4)**.** *Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group on a finite set Ω, and let $H \leq G$. Then*

$$\mu_G(H) = \sum_{K \in \mathcal{T}(H)} \mu_G(K)\, g(H,K)\,.$$

In particular,

$$|\mu_G(H)| \leq \sum_{K \in \mathcal{T}(H)} |\mu_G(K)| \cdot |g(H,K)|\,.$$

Proof. Consider a subgroup $X \leq G$ such that $X \in \mathcal{T}(H)$. Then X is transitive on Ω and obviously $X \in \overline{\mathcal{L}(X)}$. Moreover, $Y \in \mathcal{T}(H)$ and $Y \leq X$ if and only if X is the closure of Y in $\mathcal{L}(X)$. By Crapo's closure theorem we obtain

$$\sum_{Y \in \mathcal{T}(H),\, Y \leq X} \mu_Y(H) = \begin{cases} \mu_{\overline{\mathcal{L}(X)}}(H,X) & \text{if } H \in \overline{\mathcal{L}(X)} \\ 0 & \text{otherwise} \end{cases}$$

since $\mu_Y(H) = \mu_{\mathcal{L}(X)}(H,Y)$. Let $f : \mathcal{L}(G) \times \mathcal{L}(G) \to \mathbb{Z}$ be the function defined as

$$f(H,Y) = \begin{cases} \mu_Y(H) & \text{if } Y \in \mathcal{T}(H) \\ 0 & \text{otherwise} \end{cases}$$

and notice that

$$g(H,X) = \sum_{Y \in \mathcal{T}(H),\, Y \leq X} f(H,Y)\,.$$

Thus, by Möbius inversion formula (Theorem 3.1.11), we have

$$f(H,X) = \sum_{Y \in \mathcal{T}(H),\, Y \leq X} g(H,Y)\mu_X(Y)\,.$$

In the last expression, set $X = G$ and $Y = K$ to get the result. □

In [10], moreover, an upper-bound is given on the absolute value of the function g. It is interesting to notice that it is written in terms of the number of H-orbits of the set Ω, as follows.

Proposition 5.1.2 ([10], Theorem 1.5)**.** *Let G be a transitive permutation group on a set Ω, and let $H \leq G$. If $K \in \mathcal{T}(H)$ and $K \neq H$, then*

$$|g(H,K)| \leq \frac{(r!)^2}{2}$$

where r is the number of orbits of H in its natural action on Ω.

By Proposition 5.1.2, an estimation on the number of orbits r in terms of the index $|G:H|$ is useful if we are looking for a similar estimation on $|\mu_G(H)|$. Colombo and Lucchini obtain results in this direction.

Remark. Let H be a subgroup of a transitive group $G \leq \mathrm{Sym}(\Omega)$. Let $\lambda = \{\Lambda_1, \dots, \Lambda_k\}$ be the set of the orbits of H with respect to its action on Ω. Then we have that the closure of H can also be written as

$$\overline{H} = \mathrm{stab}_G(\Lambda_1) \cap \cdots \cap \mathrm{stab}_G(\Lambda_k) \tag{5.1}$$

where $\mathrm{stab}_G(\Lambda_i) = \{g \in G \mid x^g \in \Lambda_i \quad \forall x \in \Lambda_i\}$.

This remark suggests a way to define an analogue closure operator on the subgroup lattice of an irreducible subgroup of $\mathrm{GL}(V)$, for $V \simeq \mathbb{F}_q^n$.

5.1.2 Irreducible linear groups

Remark. Let G be a transitive permutation group on a finite set Ω. If H is a subgroup of G, then we could define the lattice of H-invariant subsets of Ω as

$$\mathcal{B}(\Omega, H) = \{A \subseteq \Omega \mid x^h \in A \quad \forall x \in A,\ \forall h \in H\}.$$

We notice that $\mathcal{B}(\Omega, H)$ ordered by inclusion is a boolean lattice. Indeed, if $\{\Lambda_1, \dots, \Lambda_k\}$ is the set of H-orbits on Ω, then every H-invariant subset $A \in \mathcal{B}(\Omega, H)$ is an union of orbits. In particular, $\Lambda_1, \dots, \Lambda_k$ are the atoms of $\mathcal{B}(\Omega, H)$, and the only join-irreducible elements of this lattice.

Now, let G be an irreducible subgroup of $\mathrm{GL}(n,q)$. Let $H \leq G$. We know that the lattice $\mathcal{S}(V,H)$ of H-invariant subspaces of $V \simeq \mathbb{F}_q^n$ is a finite modular lattice. Therefore, every subspace $W \in \mathcal{S}(V,H)$ can be seen as the join of some join-irreducible elements of $\mathcal{S}(V,H)$, i.e.

$$W = U_1 + \cdots + U_k$$

for some $U_1, \dots, U_k \in \mathrm{JI}(\mathcal{S}(V,H))$.

In this sense, join-irreducible elements of $\mathcal{S}(V,H)$ play the same role of orbits in $\mathcal{B}(\Omega,H)$ above. Therefore, we define a closure operator on $\mathcal{L}(G)$, for $G \leq \mathrm{GL}(n,q)$ as follows. Let G be an irreducible subgroup of G and $H \leq G$. Let

$$\mathrm{JI}(\mathcal{S}(V,H)) = \{W_1, \ldots, W_r\}$$

be the set of join-irreducible subspaces in $\mathcal{S}(V,H)$. Then, the **closure** of H in G is

$$\overline{H} = \mathrm{stab}_G(W_1) \cap \cdots \cap \mathrm{stab}_G(W_r). \tag{5.2}$$

Remark. Since every subspace in $\mathcal{S}(V,H)$ can be expressed as the sum of some join-irreducible subspaces, we have that

$$g \in \bigcap_{W \in \mathrm{JI}(\mathcal{S}(V,H))} \mathrm{stab}_G(W) \quad \Rightarrow \quad T^g = T \quad \forall T \in \mathcal{S}(V,H). \tag{5.3}$$

Therefore, we can equivalently define the closure of H in G as

$$\overline{H} = \bigcap_{W \in \mathcal{S}(V,H)} \mathrm{stab}_K(W)\,.$$

We also observe that $\mathcal{S}(V,H) = \mathcal{S}(V,\overline{H})$. Indeed, $\mathcal{S}(V,\overline{H}) \subseteq \mathcal{S}(V,H)$ since $H \subseteq \overline{H}$. Conversely, $\mathcal{S}(V,H) \subseteq \mathcal{S}(V,\overline{H})$ by (5.3).

So, we have that the function $\bar{\ }: \mathcal{L}(G) \to \mathcal{L}(G)$ is a closure operator on the subgroup lattice $\mathcal{L}(G)$, in the sense of Definition 3.1.8. A subgroup H is said to be **closed** in G if $\overline{H} = H$, and the subposet of closed subgroups in G is denoted by $\overline{\mathcal{L}(G)}$. Since G is irreducible, we have that

$$\overline{G} = \mathrm{stab}_G(0) \cap \mathrm{stab}_G(V) = G$$

and clearly $G \in \overline{\mathcal{L}(G)}$.

Similarly to the case of permutation groups, we can define

- the subset

  $$Irr_G(H) = \{K \leq G \mid H \leq K,\ K \textit{ is irreducible on } V\} \subseteq \mathcal{L}(G)$$

  of irreducible subgroups of G containing H;

- the function $g : \mathcal{L}(G) \times \mathcal{L}(G) \to \mathbb{Z}$ such that

  $$g(H,K) = \begin{cases} \mu_{\overline{\mathcal{L}(K)}}(H,K) & \text{if } K \in Irr_G(H) \text{ and } H \in \overline{\mathcal{L}(K)} \\ 0 & \text{otherwise.} \end{cases}$$

Then, for irreducible linear groups Proposition 5.1.1 assumes the following form.

Proposition 5.1.3. *Let $G \leq \mathrm{GL}(n, q)$ be an irreducible linear group on a $V \simeq \mathbb{F}_q^n$, and let $H \leq G$. Then*

$$\mu_G(H) = \sum_{K \in Irr_G(H)} \mu_G(K)\, g(H, K)\,.$$

In the next section, we apply Theorem 3.1.13 to get a similar expression for $\mu_G(H)$ by using the Möbius number of the reducible subgroup ideal $\mathcal{I}_1(G, H)$ instead of the function g. A potential advantage is that we may be able to compute $\mathcal{I}_1(G, H)$ by using Theorem 4.2.4.

5.2 Closed subgroups and the reducible subgroup ideal

Let $V \simeq \mathbb{F}_q^n$, and let G be an irreducible subgroup of $\mathrm{GL}(V)$. We recall that

$$\mathcal{C}_1(G, H) = \{\, \mathrm{stab}_G(W) \mid 0 < W < V\,,\ H \subseteq \mathrm{stab}_G(W)\,\}$$

is the first class of Aschbacher restricted to the subgroups containing H. The ideal generated by $\mathcal{C}_1(G, H)$ in $\mathcal{L}(G)_{\geq H}$ is

$$\mathcal{I}_1(G, H) = \{K \leq G \mid H \leq K \leq M \text{ for some } M \in \mathcal{C}_1(G, H)\}$$

Moreover we have

$$\widehat{\mathcal{I}}_1(G, H) = \mathcal{I}_1(G, H) \cup \{H, G\}.$$

In particular, if H is a reducible subgroup of G, then $H \in \mathcal{I}_1(G, H)$ and

$$\widehat{\mathcal{I}}_1(G, H) = \mathcal{I}_1(G, H) \cup \{G\}.$$

Both $\mathcal{I}_1(G, H)$ and $\widehat{\mathcal{I}}_1(G, H)$ are subposets of $\mathcal{L}(G)$.

Now, for any irreducible subgroup K of G, we can similarly define

- $\mathcal{C}_1(K, H) = \{\, \mathrm{stab}_K(W) \mid 0 < W < V\,,\ H \subseteq \mathrm{stab}_K(W)\,\}$;
- $\mathcal{I}_1(K, H) = \{L \leq K \mid H \leq L \leq M \text{ for some } M \in \mathcal{C}_1(K, H)\}$;
- $\widehat{\mathcal{I}}_1(K, H) = \mathcal{I}_1(K, H) \cup \{H, K\}$.

Remark. If W is a non-trivial subspace of V, then we have

$$\mathrm{stab}_K(W) \subseteq \mathrm{stab}_G(W).$$

Therefore, if $X \in \mathcal{I}_1(K, H)$, then $X \in \mathcal{I}_1(G, H)$ and

$$\mathcal{I}_1(K, H) = \{X \in \mathcal{I}_1(G, H) \mid X < K\}. \tag{5.4}$$

In Chapter 3, we have proven Theorem 3.1.13, that allows us to express the Möbius function of a finite lattice L in terms of the Möbius number of an order ideal I. We need to recall Theorem 3.1.13 for the notation, and then we apply it to give $\mu_G(H)$ in terms of the reducible subgroup ideal $\mathcal{I}_1(G,H)$.

Theorem (3.1.13). *Let L be a finite lattice with minimum $\hat{0}$ and maximum $\hat{1}$, and let $I \subseteq L$ be an order ideal of L. Let $\widehat{I} = I \cup \{\hat{1}\}$. Then*

$$\mu_L(\hat{0},\hat{1}) = \mu_{\widehat{I}}(\hat{0},\hat{1}) + \sum_{y \in L \setminus \widehat{I}} \mu_{\widehat{I}_{<y}}(\hat{0},y) \cdot \mu_L(y,\hat{1}) \tag{5.5}$$

where $\widehat{I}_{<y} = \{x \in I \mid x < y\} \cup \{y\}$.

In our case, the lattice is $\mathcal{L}(G)_{\geq H}$, with minimum H and maximum G. The ideal is obviously $\mathcal{I}_1(G,H)$, and we focus on

$$\widehat{\mathcal{I}_1}(G,H)_{<K}$$

for $K \in \mathcal{L}(G)_{\geq H} \setminus \widehat{\mathcal{I}_1}(G,H)$. But this is equivalent to requiring that K is an irreducible proper subgroup of G, hence

$$\widehat{\mathcal{I}_1}(G,H)_{<K} = \{X \in \mathcal{I}_1(G,H) \mid X < K\} = \mathcal{I}_1(K,H)$$

as in (5.4).

Then we have the following.

Theorem 5.2.1. *Let G be an irreducible subgroup of* $\mathrm{GL}(n,q)$. *Let H be a subgroup of G. Then*

$$\mu(H,G) = \mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G) + \sum_{\substack{K \notin \mathcal{I}_1(G,H) \\ H<K<G}} \mu(K,G) \cdot \mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K)\,.$$

Remark. Since $\mu(G,G) = 1$ and G is irreducible, Theorem (5.2.1) is equivalent to saying that

$$\mu(H,G) = \sum_{K \notin \mathcal{I}_1(G,H)} \mu(K,G) \cdot \mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K) \tag{5.6}$$

where the term $\mu_{\widehat{\mathcal{I}}_1(G,H)}(H,G)$ is equal to

$$\mu(K,G) \cdot \mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K)$$

for $K = G$.

If we denote by $Irr_G(H)$ the set of irreducible subgroups of G that contain H, then we can finally write (5.6) as

$$\mu(H,G) = \sum_{K \in Irr_G(H)} \mu(K,G) \cdot \mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K)\,. \tag{5.7}$$

In Chapter 4, we have computed $\mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K)$ and by Theorem 4.2.4 we know that

$$-\mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K) = \sum_{E\in\Psi'(K,H)} (-1)^{|E|} \tag{5.8}$$

where

$$\Psi'(K,H) = \{E \subseteq \mathcal{S}(V,H)^* \mid \bigcap_{W\in E} \mathrm{stab}_K(W) \neq H\}.$$

We can try to use expression (5.8) of $\mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K)$ in order to find some bound on its absolute value in terms of the number of join-irreducible elements in $\mathcal{S}(V,H)$, as in Proposition 5.1.2 with respect to $g(H,K)$ and the orbits of H. A first approximation is the following.

Proposition 5.2.2. *Let G be an irreducible subgroup of* $\mathrm{GL}(V)$*, with $V \simeq \mathbb{F}_q^n$. Let $H \leq G$. If $K \in Irr_G(H)$, then*

$$\left|\mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K)\right| \leq 2^{2^r}. \tag{5.9}$$

where $r = |\mathrm{JI}(\mathcal{S}(V,H))|$ is the number of join-irreducible elements of $\mathcal{S}(V,H)$.

Proof. By (5.8), we have that

$$\left|\mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K)\right| = \left|\sum_{E\in\Psi'(K,H)} (-1)^{|E|}\right| \leq 2^{|\Psi'(K,H)|} \leq 2^{|\mathcal{S}(V,H)|}.$$

Since every element of $\mathcal{S}(V,H)$ is a join of some join-irreducible elements, $|\mathcal{S}(V,H)| \leq 2^r$. ☐

Actually, it would be interesting to find some estimates of this value in terms of the index $|G : H|$. Maybe a better approximation in terms of the join-irreducible elements is necessary.

In the following proposition, we have a remarkable property of subgroups which are not closed in an irreducible subgroup $K \leq \mathrm{GL}(n,q)$.

Proposition 5.2.3. *Let $H \leq G$ and $K \in Irr_G(H)$. If H is not closed in K, then*

$$\mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K) = 0.$$

Proof. Let $W_1,\dots,W_r$ be the join-irreducible elements of $\mathcal{S}(V,H)$. Assume that H is not closed in K. Then

$$H \subsetneq \bigcap_{i=1}^{r} \mathrm{stab}_K(W_i)$$

and we have that

$$H \subsetneq \bigcap_{W \in E} \mathrm{stab}_K(W) \quad \forall\, E \subseteq \mathcal{S}(V,H)^*,\, E \neq \emptyset\,.$$

Thus, if H is not closed in K, by definition of $\Psi'(K,H)$ we have that

$$E \subseteq \mathcal{S}(V,H)^* \quad \Rightarrow \quad E \in \Psi'(K,H)\,.$$

So,

$$\sum_{E \in \Psi'(K,H)} (-1)^{|E|} = 0\,.$$

□

We will apply this result in §5.3 to prove Proposition 5.3.2.

5.3 The number of closed subgroups

Now we are interested in the number of closed subgroups in $\mathrm{GL}(n,q)$. A motivation can be found in part *(ii)* of Conjecture 3.2.10, as follows. For $m \in \mathbb{N}$, let $b_m(G)$ the number of subgroups of G such that $|G:H| = m$ and $\mu_G(H) \neq 0$. We would like to estimate the growth of $b_m(G)$ with respect to m and give a polynomial bound

$$b_m(G) \leq m^{\alpha} \quad \forall\, m \in \mathbb{N}$$

for all $G = \mathrm{GL}(n,q)$, such that the constant α is independent of n and q. Such a polynomial bound can be applied to Conjecture 3.2.10, if the considered almost-simple groups are $\mathrm{PGL}(n,q)$.

Conjecture 5.3.1. *Let $G = \mathrm{PGL}(n,q)$. Then there exists an absolute constant α, independent of n and q, such that*

$$b_m(G) \leq m^{\alpha} \quad \forall\, m \in \mathbb{N}$$

where

$$b_m(G) = \#\{H \leq G \mid |G:H| = m \;\; \textit{and} \;\; \mu(H,G) \neq 0\}\,.$$

The following proposition is useful because it reduces the problem to estimating the number of closed subgroups and the number of irreducible ones.

Remark. We notice that a closure operator can be defined also for the subgroup lattice of $\mathrm{PGL}(n,q)$ in the same way as we defined the one for $\mathrm{GL}(n,q)$. Our results are actually given for $\mathrm{GL}(n,q)$, but it is not difficult to obtain the analogue for the quotient $\mathrm{GL}(n,q)/Z(\mathrm{GL}(n,q))$, since the centre $Z(\mathrm{GL}(n,q))$ is contained in every closed subgroup of $\mathrm{GL}(n,q)$.

Proposition 5.3.2. *Let G be an irreducible subgroup of $\mathrm{GL}(n,q)$, and let $H \leq G$. If $\mu_G(H) \neq 0$, then there exist a subgroup $K \in Irr_G(H)$ and a closed subgroup C in G such that $H = K \cap C$.*

Proof. Let $H \leq G$ such that $\mu_G(H) \neq 0$. We know that

$$\mu_G(H) = \sum_{K \in Irr_G(H)} \mu(K,G) \cdot \mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K)\,.$$

Therefore $\mu_G(H) \neq 0$ implies that there exists a subgroup $K \in Irr_G(H)$ such that

$$\mu(K,G)\mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K) \neq 0.$$

Then we have that $\mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K) \neq 0$. By Proposition 5.2.3, we conclude that H is closed in K.
If H is closed in K, then there exists a closed subgroup C in G such that $H = K \cap C$. Indeed

$$H = \bigcap_{W \in \mathcal{S}(V,H)} \mathrm{stab}_K(W) = K \cap \bigcap_{W \in \mathcal{S}(V,H)} \mathrm{stab}_G(W)\,.$$

□

By Proposition 5.3.2, in order to prove Conjecture 5.3.1 we need that the two following conditions hold:

- the number

$$\#\{K \leq G \mid K \in Irr_G(H),\ \mu_G(K) \neq 0,\ |G:K| \text{ divides } m\}$$

  is polynomially bounded by the index $m = |G:H|$;
- the number of closed subgroups in G of index dividing $m = |G:H|$ is polynomially bounded by m.

In view of Conjecture 3.2.10, one could be interested in estimating the number of closed subgroups in $\mathrm{GL}(n,q)$. In §5.3.1, we concentrate on the number of closed subgroups H in $\mathrm{GL}(n,q)$ such that the lattice $\mathcal{S}(V,H)$ is isomorphic to a product of chains. An example for this kind of subgroups is represented by the closure of the subgroup generated by a cyclic matrix in $\mathrm{GL}(n,q)$.

5.3.1 Closure of subgroups generated by cyclic matrices

In this section, we prove that there is a polynomial bound, with respect to the index $|G:H| = m$, on the growth of the number of closed subgroups $H \leq \mathrm{GL}(n,q)$ such that the lattice $\mathcal{S}(V,H)$ is isomorphic to a product of chains. This is the case, for example, when H is the subgroup generated by a cyclic matrix in $\mathrm{GL}(n,q)$. In particular we have the following theorem.

Theorem 5.3.3. *Let $V \simeq \mathbb{F}_q^n$ and $G = \mathrm{GL}(n, q)$. Let*

$$c_m^{prod}(G) = \#\{H \le G \mid H = \overline{H},\ \mathcal{S}(V, H) \text{ is a product of chains, } |G : H| = m\}.$$

Then there exists an absolute constant α, independent of n and q, such that

$$c_m^{prod}(G) \le m^{\alpha} \quad \forall\, m \in \mathbb{N}\,.$$

The proof in divided into three parts. At first we consider only closed subgroups H of G such that the lattice of H-invariant subspaces of V is boolean. Then we study the same, but for closed subgroups H of G such that $\mathcal{S}(V, H)$ is a flag (i.e. a chain of subspaces) in V. Finally, we can combine the previous results to prove Theorem 5.3.3.

Notation. We will consider the following three sets:

(a) $\mathcal{F}_m^{bool}(G)$ is the set of closed subgroups $H \le G$ such that $|G : H| = m$ and the lattice $\mathcal{S}(V, H)$ is boolean.

(b) $\mathcal{F}_m^{flag}(G)$ is the set of closed subgroups $H \le G$ such that $|G : H| = m$ and the lattice $\mathcal{S}(V, H)$ is a flag.

(c) $\mathcal{F}_m^{prod}(G)$ is the set of closed subgroups $H \le G$ such that $|G : H| = m$ and the lattice $\mathcal{S}(V, H)$ is isomorphic to a product of chains.

The case of $\mathcal{F}_m^{bool}(G)$

In this case, the lattice $\mathcal{S}(V, H)$ is boolean. In other terms, by Corollary 2.2.17, it is isomorphic to a product of r chains of length 1. We want to prove Proposition 5.3.4 in order to say that the number of closed subgroups H in $\mathrm{GL}(n, q)$ such that $|G : H| = m$ and $\mathcal{S}(V, H)$ boolean is polynomially bounded by m, independently of n and q. Firstly, we recall some notions about the q**-binomial coefficient**.

Remark. We denote by $\binom{n}{x}_q$ the q-analogue of the binomial coefficient $\binom{n}{x}$. It means that

$$\binom{n}{x}_q = \frac{[n]_q!}{[x]_q!\,[n-x]_q!} \tag{5.10}$$

where

$$[z]_q! = \frac{(q^z - 1)\cdot \ldots \cdot (q-1)}{(q-1)^z}. \tag{5.11}$$

Both (5.10) and (5.11) descend from the definition of $[z]_q$ as

$$[z]_q = 1 + q + q^2 + \cdots + q^{z-1} = \frac{(q^z - 1)}{(q-1)}\,.$$

If $V = \mathbb{F}_q^n$ and x is a positive integer $\leq n$, it is known that $\binom{n}{x}_q$ represents the number of subspaces of V of dimension x.

We know, moreover, that $|\mathrm{GL}(n,q)| = (q^n - 1) \cdot \ldots \cdot (q-1)\, q^{\binom{n}{2}}$, which can be also written as

$$|\mathrm{GL}(n,q)| = [n]_q!(q-1)^n\, q^{\binom{n}{2}} \tag{5.12}$$

by using (5.10).

So, finally, let $V \simeq \mathbb{F}_q^n$ and $W_1, W_2 \leq V$ such that $V = W_1 \oplus W_2$. Let

$$H = \mathrm{GL}(W_1) \oplus \mathrm{GL}(W_2).$$

We use the q-binomial coefficient to express the index of H in $G = \mathrm{GL}(n,q)$. In particular, if $x_1 = \dim(W_1)$ and $x_2 = \dim(W_2)$, we have $x_2 = n - x_1$. Then

$$\frac{|\mathrm{GL}(V)|}{|\mathrm{GL}(W_1)| \cdot |\mathrm{GL}(W_2)|} = \frac{[n]_q!(q-1)^n\, q^{\binom{n}{2}}}{[x_1]_q!(q-1)^{x_1}\, q^{\binom{x_1}{2}} [n-x_1]_q!(q-1)^{n-x_1}\, q^{\binom{n-x_1}{2}}}$$

$$= \binom{n}{x_1}_q \cdot q^{\binom{n}{2} - \binom{x_1}{2} - \binom{n-x_1}{2}}$$

$$= \binom{n}{x_1}_q \cdot q^{x_1(n-x_1)}\,. \tag{5.13}$$

We can use (5.13) to prove the following Proposition 5.3.4. Actually, its proof is similar to the proof of [10, Lemma 2.3]. This is quite natural, since the lattice $\mathcal{B}(\Omega, H)$ considered (implicitly) by Colombo and Lucchini for permutation groups is boolean, as we have observed at the beginning of §5.1.2.

Proposition 5.3.4. *Let* $G = \mathrm{GL}(n,q)$ *and*

$$c_m^{bool}(G) = \#\mathcal{F}_m^{bool}(G).$$

Then there exists an absolute constant α_1*, independent of* n *and* q*, such that*

$$c_m^{bool}(G) \leq m^{\alpha_1} \quad \forall\, m \in \mathbb{N}\,.$$

Proof. Let $V \simeq \mathbb{F}_q^n$ and let H be a closed subgroup of $G = \mathrm{GL}(V)$ such that H is closed in G. Then

$$H = \bigcap_{i=1}^{r} \mathrm{stab}_G(W_i)$$

where $\mathrm{JI}(\mathcal{S}(V,H)) = \{W_1,\ldots,W_r\}$ is the set of join-irreducible elements in $\mathcal{S}(V,H)$. If $\mathcal{S}(V,H)$ is boolean, then $W_1,\ldots,W_r$ are the atoms of $\mathcal{S}(V,H)$ and, in particular, $V = \bigoplus_{i=1}^r W_i$. Then

$$H = \bigcap_{i=1}^{r} \mathrm{stab}_G(W_i) = \mathrm{GL}(W_1) \oplus \cdots \oplus \mathrm{GL}(W_r),$$

with $|H| = |\mathrm{GL}(W_1)| \cdot \ldots \cdot |\mathrm{GL}(W_r)|$.
Let $x_i = \dim W_i$ for all $i = 1,\ldots,r$ and let $m = |G : H|$. We can inductively use (5.13) to obtain that

$$m = |G:H| = \frac{|\mathrm{GL}(V)|}{|\mathrm{GL}(W_1)| \cdot \ldots \cdot |\mathrm{GL}(W_r)|}$$

$$= \binom{n}{x_1}_q \cdot \binom{n-x_1}{x_2}_q \cdot \ldots \cdot \binom{n-x_1-\ldots-x_{r-2}}{x_{r-1}}_q \cdot q^{\epsilon}$$

where the exponent

$$\epsilon := \epsilon(n,x_1,\ldots,x_{r-1}) = x_1(n-x_1) + x_2(n-x_1-x_2) + \ldots + x_{r-1}x_r$$

depends only on $n, x_1,\ldots,x_{r-1}$. Let

$$v_1 = \binom{d}{x_1}_q, \quad v_i = \binom{d-x_1-\ldots-x_{i-1}}{x_i}_q \text{ for } i = 2,\ldots,r-1, \quad v_r = q^{\epsilon}$$

so that $m = v_1 \cdot \ldots \cdot v_r$. By [20], the number of such ordered factorizations of m is at most m^2. If we fix the factorization $m = v_1 \cdot \ldots \cdot v_r$, then for all $i = 1,\ldots,r-1$ there are at most two possible values of x_i for which we have v_i, and v_r is uniquely determined by the previous v_i. So, for every fixed ordered factorization, we have at most 2^{r-1} possibilities, and $2^{r-1} \le m$. Then there are at most m^3 choices of $x_1,\ldots,x_r$ giving the same m. Hence there are at most m^3 conjugacy classes of closed subgroups H with index m such that $\mathcal{S}(V,H)$ is boolean. Each of these subgroups has at most m conjugates, so $c_m^{bool}(G) \le m^4$. □

The case of $\mathcal{F}_m^{flag}(G)$

Similarly to Proposition 5.3.4, we want to prove that the number of closed subgroups H in $\mathrm{GL}(n,q)$, such that $|G : H| = m$ and $\mathcal{S}(V,H)$ is a flag, is polynomially bounded by m, independently of n and q. Here we follow [45] for notation and remarks about flags of subspaces.

Let $V \simeq \mathbb{F}_q^n$ be a finite vector space of dimension d over $\mathbb{F}_q$. A **flag** f on V is a sequence $(0, W_1,\ldots,W_k,V)$ of subspaces of V such that

$$0 < W_1 < \cdots < W_k < V.$$

Moreover, we say that $f = (0, W_1, \dots, W_k, V)$ is a **flag of type** $(d_1, \dots, d_k)$, where $d_i := \dim(W_i)$ for all $i = 1, \dots, k$.

Remark. A flag f on V can be also regarded as a subposet of the subspace lattice of V. In particular, f is a chain of subspaces from 0 to V, ordered by inclusion.

If $k = n-1$, so that $d_1 = 1$ and $d_{i+1} = d_i + 1$ for all i, then the chain from 0 to V has length n, and the flag is called **complete**.

Let Fl_V be the set of all flags on V. The group $G = \mathrm{GL}(V)$ acts on Fl_V in the obvious way:

$$(0, W_1, \dots, W_k, V)^g = (0, W_1^g, \dots, W_r^g, V) \quad \forall\, g \in G.$$

In particular, with some abuse of notation, we have that the stabilizer of a flag $f = (0, W_1, \dots, W_k, V)$ is

$$\mathrm{stab}_G(f) = \{g \in G \mid W_i^g = W_i \quad \forall\, i = 1, \dots, k\} = \bigcap_{i=1}^{k} \mathrm{stab}_G W_i.$$

where $\mathrm{stab}_G W_i$ also denotes the stabilizer in G of W_i with respect to the usual action of G on the subspace lattice of V. So, for us $\mathrm{stab}_G(W_i)$ is an equivalent way to write $\mathrm{stab}_G(0, W_i, V)$.

The stabilizer in G of a flag on V is also called a **parabolic subgroup** of $\mathrm{GL}(V)$. In particular, if the flag is complete we say that it is a **maximal parabolic subgroup**. We remind the following fact.

Proposition 5.3.5. *A subgroup $P \leq \mathrm{GL}(V)$ is parabolic if and only if it is closed in* $\mathrm{GL}(V)$ *and $\mathcal{S}(V, P)$ is a flag on V.*

Proof. On one side, the implication is trivial by definition. On the other side, the implication is a consequence of Bruhat decomposition (see for instance [5]). □

Let $V \simeq \mathbb{F}_q^d$ and let

$$0 < d_1 < \cdots < d_k < d$$

be a sequence of positive integers. We set

$$Fl_V(d_1, \dots, d_k) = \{f \text{ flag on } V \mid f \text{ is of type } (d_1, \dots, d_k)\}.$$

We observe that $\mathrm{GL}(V)$ acts transitively on $Fl_V(d_1, \dots, d_k)$ and, consequently, the stabilizers of flags in $Fl_V(d_1, \dots, d_k)$ are conjugate to each other.

So, we have the following proposition.

Proposition 5.3.6. *Let $G = \mathrm{GL}(n,q)$ and*

$$c_m^{flag}(G) = \#\mathcal{F}_m^{flag}(G).$$

Then there exists an absolute constant α_2, independent of n and q, such that

$$c_m^{flag}(G) \leq m^{\alpha_2} \quad \forall\, m \in \mathbb{N}\,.$$

Remark. By Proposition 5.3.5, $c_m^{flag}(G)$ is the number of parabolic subgroups of index m in G.

Proof. Let H be a parabolic subgroup of $G = \mathrm{GL}(V)$, $V \simeq \mathbb{F}_q^d$. Then H is the stabilizer of a flag f:

$$0 < W_1 < \cdots < W_k < V,$$

so that

$$H = \mathrm{stab}_G(f) = \bigcap_{i=1}^{r} \mathrm{stab}_G(W_i),$$

where $\{W_1, \ldots, W_k\} = \mathrm{JI}(\mathcal{S}(V,C))$ is the set of join-irreducible elements of $\mathcal{S}(V,H)$. Let $x_i = \dim W_i$ for all $i = 1, \ldots, k$ and let $m = |G : H|$. Consider the set of all flags of type $(x_1, \ldots, x_k)$ on V, denoted by $Fl_V(x_1, \ldots, x_k)$. Since the action of G on $Fl_V(x_1, \ldots, x_k)$ is transitive, we have that

$$|Fl_V(x_1, \ldots, x_k)| = \frac{|\mathrm{GL}(V)|}{|\mathrm{stab}_G(f)|}\,.$$

But we can also compute $|Fl_V(x_1, \ldots, x_k)|$ as follows:

$$\begin{aligned} |Fl_V(x_1, \ldots, x_k)| &= |Fl_V(x_k)| \cdot |Fl_{W_k}(x_1, \ldots, x_{k-1})| \\ &= |Fl_V(x_k)| \cdot |Fl_{W_k}(x_{k-1})| \cdot \ldots \cdot |Fl_{W_2}(x_1)| \\ &= \binom{d}{x_k}_q \cdot \binom{x_k}{x_{k-1}}_q \cdot \ldots \cdot \binom{x_2}{x_1}_q . \end{aligned}$$

by using the q-binomial coefficient. Then we have

$$m = |G : H| = |Fl_V(x_1, \ldots, x_k)| = \binom{d}{x_k}_q \cdot \binom{x_k}{x_{k-1}}_q \cdot \ldots \cdot \binom{x_2}{x_1}_q .$$

Let

$$v_k = \binom{d}{x_k}_q, \quad v_i = \binom{x_{i+1}}{x_i}_q \quad \text{for } i = 1, \ldots, k-1$$

so that $m = v_k \cdot \ldots \cdot v_1$. As in the proof of Proposition 5.3.4, we know that the number of such ordered factorizations of m is at most m^2 by [20]. Moreover, if we fix the factorization $m = v_k \cdot \ldots \cdot v_1$, for all $i = 1, \ldots, k$ there are at most two possible values of x_i for which we have v_i, and v_k is uniquely determined by the previous v_i. So, for every fixed ordered factorization, we have at most 2^k possibilities, and $2^k \leq m$. Then there are at most m^3 choices of $x_1, ..., x_k$ giving the same m. Hence there are at most m^3 conjugacy classes of closed subgroups H with index m such that $\mathcal{S}(V, H)$ is a flag. Each of these parabolic subgroups has at most m conjugates, so $c_m^{flag}(G) \leq m^4$. □

The case of $\mathcal{F}_m^{prod}(G)$

Here we use together Proposition 5.3.4 and Proposition 5.3.6 in order to prove Theorem 5.3.3, that we write again here below. The assumption now is that $\mathcal{S}(V, H)$ is a product of chains.

Theorem (5.3.3). *Let* $G = \mathrm{GL}(n, q)$ *and*

$$c_m^{prod}(G) = \#\mathcal{F}_m^{prod}(G).$$

Then there exists an absolute constant α*, independent of* n *and* q*, such that*

$$c_m^{prod}(G) \leq m^{\alpha} \quad \forall\, m \in \mathbb{N}\,.$$

Proof. Let $V \simeq \mathbb{F}_q^d$ and let H be a closed subgroup of $G = \mathrm{GL}(V)$. We assume that $\mathcal{S}(V, H)$ is isomorphic to a product of r chains $\gamma_1, \ldots, \gamma_r$. For all $i = 1, \ldots, r$, let $W_{k_i}^{(i)}$ be the maximum of γ_i, so that $k_i = \dim(W_{k_i}^{(i)})$. Then, each γ_i is a flag on $W_{k_i}^{(i)}$ of the form:

$$0 = W_0^{(i)} < W_1^{(i)} < \cdots < W_{k_i - 1}^{(i)} < W_{k_i}^{(i)}$$

and every subspace $T \in \mathcal{S}(V, H)$ can be identified with a r-tuple of subspaces $(W_{j_1}^{(1)}, \ldots, W_{j_r}^{(r)}) \in \prod_{i=1}^r \gamma_i$, so that $j_i \in \{0, \ldots, k_i\}$ and

$$T = \bigoplus_{i=1}^{r} W_{j_i}^{(i)}\,.$$

In particular,

$$V = \bigoplus_{i=1}^{r} W_{k_i}^{(i)}\,. \tag{5.14}$$

The set $\mathrm{JI}(\mathcal{S}(V, H))$ of the join-irreducible elements in $\mathcal{S}(V, H)$ coincides with the union of the chains:

$$\mathrm{JI}(\mathcal{S}(V, H)) = \bigcup_{i=1}^{r} \gamma_i\,.$$

It means that every join-irreducible element of $\mathcal{S}(V,H)$ is one of the $W_j^{(i)}$, with $i \in \{1,\dots,r\}$ and $j \in \{1,\dots,k_i\}$, and it can be identified with a r-tuple of the form $(0,\dots,0,W_j^{(i)},0,\dots,0) \in \prod_{s=1}^r \gamma_s$ such that $W_j^{(i)} \in \gamma_i$. Since H is closed, H is uniquely determined by the join-irreducible elements of $\mathcal{S}(V,H)$ in the following way:

$$H = \bigcap_{W \in \mathrm{JI}(\mathcal{S}(V,H))} \mathrm{stab}_G(W) = \bigcap_{i=1}^{r} \bigcap_{j=1}^{k_i} \mathrm{stab}_G(W_j^{(i)})\,. \tag{5.15}$$

Let $|G:H| = m$. Then, as we have seen in the proof of Proposition 5.3.4, for each divisor $\overline{m}$ of m we have at most $\overline{m}^4$ decompositions of V as in (5.14) such that

$$\overline{m} = \frac{|\mathrm{GL}(V)|}{|\bigcap_{i=1}^r \mathrm{stab}_G(W_{k_i}^{(i)})|}\,.$$

Thus, we have at most m^5 such decompositions of V.
Now we fix one of these decompositions: $V = \bigoplus_{i=1}^r W_{k_i}^{(i)}$. For all $i = 1,\dots,r$ we can consider the relative chain $C_i = \gamma_i \cup \{V\}$ given by

$$0 = W_0^{(i)} < W_1^{(i)} < \dots < W_{k_i-1}^{(i)} < W_{k_i}^{(i)} < V$$

such that

$$\frac{|\mathrm{GL}(V)|}{|\mathrm{stab}_G(C_i)|} = \binom{n}{x_{k_i}}_q \cdot \binom{x_{k_i}}{x_{k_i-1}}_q \cdot \dots \cdot \binom{x_2}{x_1}_q .$$

where $x_j = \dim(W_j^{(i)})$ for each $j = 1,\dots,k_i$. We observe that

$$\binom{n}{x_{k_i}}_q = \frac{|\mathrm{GL}(V)|}{|\mathrm{stab}_G(W_{k_i}^{(i)})|}$$

has been fixed with the decomposition of V, so that we have

$$y_i = \frac{|\mathrm{GL}(V)|}{|\mathrm{stab}_G(C_i)|} \cdot \frac{|\mathrm{stab}_G(W_{k_i}^{(i)})|}{|\mathrm{GL}(V)|}$$

$$= \frac{|\mathrm{stab}_G(W_{k_i}^{(i)})|}{|\mathrm{stab}_G(C_i)|} = \binom{x_{k_i}}{x_{k_i-1}}_q \cdot \dots \cdot \binom{x_2}{x_1}_q . \tag{5.16}$$

As in the proof of Proposition 5.3.6, there are at most y_i^4 ways to choose the chain C_i, for all $i = 1,\dots,r$.
Now, we observe that

$$y_i = \frac{|\mathrm{stab}_G(W_{k_i}^{(i)})|}{|\mathrm{stab}_G(C_i)|} = \frac{|\mathrm{GL}(W_{k_i}^{(i)})|}{|\mathrm{stab}_{\mathrm{GL}(W_{k_i}^{(i)})}(\gamma_i)|} \tag{5.17}$$

and that

$$m = |G : H| = \frac{|\mathrm{GL}(V)|}{|\mathrm{stab}_{\mathrm{GL}(W_{k_1}^{(1)})}(\gamma_1)| \cdot \ldots \cdot |\mathrm{stab}_{\mathrm{GL}(W_{k_r}^{(r)})}(\gamma_r)|}\,. \qquad (5.18)$$

So, by Equations (5.17) and (5.18), we obtain that

$$m \geq \frac{|\mathrm{GL}(W_{k_1}^{(1)})|}{|\mathrm{stab}_{\mathrm{GL}(W_{k_1}^{(1)})}(\gamma_1)|} \cdot \ldots \cdot \frac{|\mathrm{GL}(W_{k_r}^{(r)})|}{|\mathrm{stab}_{\mathrm{GL}(W_{k_r}^{(r)})}(\gamma_r)|} = y_1 \cdot \ldots \cdot y_r\,,$$

hence $y_1^4 \cdot \ldots \cdot y_r^4 \leq m^4$ is an upper bound on the number of chains, if we have fixed $y_1, \ldots, y_r$. But now we see that $y_1 \cdot \ldots \cdot y_r$ is a factorization of a divisor d of m. By [20], there are at most d^2 such factorizations for all d, so that we can choose at most m^3 factorizations $y_1 \cdot \ldots \cdot y_r$, after we have fixed the decomposition of $V = \bigoplus_{i=1}^r W_{k_i}^{(i)}$.
Finally, we have that

$$c_m^{prod}(G) \leq m^5 \cdot m^4 \cdot m^3 = m^{12}.$$

□

Some final comments

Many arguments of this thesis give us only partial results. We list here some possible hints for future research.

1. By Theorem 5.3.3, we have a polynomial bound in m

$$z_m \leq m^\alpha \quad \text{for all } m \in \mathbb{N}$$

on the number z_m of closed subgroups of index m in $\mathrm{GL}(n, q)$ that are the closure of subgroups generated by cyclic matrices. Indeed, if ξ is a cyclic matrix of $\mathrm{GL}(n, q)$, then $\mathcal{S}(V, H)$ is isomorphic to a product of chains if $H = \langle \xi \rangle$. And $\mathcal{S}(V, \overline{H}) = \mathcal{S}(V, H)$.

We can also notice that in general the subgroup generated by a cyclic matrix is not closed in $\mathrm{GL}(n, q)$. For instance, let

$$\xi = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

be the companion matrix in $\mathrm{GL}(3, 5)$ of the polynomial

$$t^3 - 1 = (t-1)(1 + t + t^2) \in \mathbb{F}_5[t]\,.$$

Then $H = \langle \xi \rangle$ has order 3, but

$$\overline{H} \simeq \mathrm{GL}(1, 5) \oplus \mathrm{GL}(2, 5).$$

However, in general, these are not the only closed subgroups of $\mathrm{GL}(n, q)$. The following are worth to be studied.

- To find a similar estimate on the number of closed subgroups K that contain some cyclic matrix. In this case, $\mathcal{S}(V,K)$ is a sublattice of a product of chains.
- In view of Proposition 5.3.2, it is also important to obtain information about the structure of closed subgroups which do not contain cyclic matrices and some estimates on their proportion among all closed subgroups of $\mathrm{GL}(n,q)$.

2. In §5.2, we have motivated the relevance of the Möbius number

$$\mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K) \tag{5.19}$$

of the ideal $\mathcal{I}_1(K,H)$, for an irreducible subgroup $K \leq G$ containing H. Here some comments about it.

- By Proposition 5.2.3, if H is not closed in K, then

$$\mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K) = 0.$$

If H is closed in G, we have presented in §4.5 some methods to compute (5.19), or at least estimate it. In general, by Theorem 4.2.4,

$$\mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K) = \sum_{E\in\Psi'(K,H)} (-1)^{|E|}. \tag{5.20}$$

- In Proposition 5.2.2, we have given a possible bound to the absolute value of (5.20), in terms of the number r of join-irreducible elements in $\mathcal{S}(V,H)$. The number r does not depend on the irreducible subgroup K.

In general, by Proposition 4.4.3, if for every $E \in \Gamma(V,H)$ there exists an element $x \in K$ such that

$$x \in \bigcap_{W\in E} \mathrm{stab}_K(W) \ \text{ but } x \notin H, \tag{5.21}$$

then $\Gamma(V,H) \subseteq \Psi'(K,H)$ and

$$\sum_{E\in\Psi'(K,H)\cap\Gamma(V,H)} (-1)^{|E|} = \sum_{E\in\Gamma(V,H)} (-1)^{|E|}. \tag{5.22}$$

By Corollary 4.4.2, if $\mathcal{S}(V,H)$ is distributive and has prime rank, then

$$\sum_{E\in\Psi'(K,H)} (-1)^{|E|} = \sum_{E\in\Psi'(K,H)\cap\Gamma(V,H)} (-1)^{|E|}. \tag{5.23}$$

It is interesting to characterize subgroups $H \leq K \leq G$ such that $\mathcal{S}(V,H)$ is **distributive of prime rank**, when there exists an element $x \in K$ as in (5.21). If such an element exists for all $E \in \Gamma(V,H)$, then by Equations (5.20), (5.22), and (5.23), and by Theorem 4.4.5 we have that

$$\mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K) = \sum_{E \in \Psi'(K,H)} (-1)^{|E|} = \sum_{E \in \Gamma(V,H)} (-1)^{|E|}.$$

3. By using

$$\mu_G(H) = \sum_{K \in Irr_G(H)} \mu_G(K) \cdot \mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K)\,, \tag{5.24}$$

we should investigate how many terms in the sum 5.24 are equal to 0. This is the case if $\mu_{\widehat{\mathcal{I}}_1(K,H)}(H,K) = 0$ or $\mu_G(K) = 0$. In order to bound the absolute value $|\mu_G(H)|$ in terms of the index $|G : H|$, we also need estimates on the number of irreducible subgroups in $\mathrm{GL}(n,q)$ and on $|\mu_G(K)|$ for an irreducible subgroup of G.

Bibliography

[1] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Inventiones Mathematicae*, **76** (1984), 469-514.

[2] M. Aschbacher, *Finite Group Theory*, Cambridge University Press, Cambridge, 1986.

[3] Kenneth Baclawski, Galois Connections and the Leray Spectral Sequence, *Advances in Mathematics*, **25** (1977), 191-215.

[4] T.S. Blyth, *Lattices and Ordered Algebraic Structures*, Springer-Verlag, London, 2005.

[5] Armand Borel, *Linear Algebraic Groups* (second ed.), Springer-Verlag, New York, 1991 (first ed. published by W.A. Benjamin, Inc., 1969)

[6] John Bray, Derek Holt and Colva Roney-Dougal, *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*, Cambridge University Press, Cambridge, 2013

[7] L. Brickman and P. A. Fillmore, The Invariant Subspace Lattice of a Linear Transformation, *Canadian Journal of Mathematics* **19** (1967), 810-822.

[8] Scott Brown, *Finite Reducible Matrix Algebras*, Ph.D. Thesis, The University of Western Australia, 2006.

[9] Peter J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, Cambridge, 1994.

[10] Valentina Colombo and Andrea Lucchini, On the subgroups with non-zero Möbius numbers in the alternating and symmetric groups, *Journal of Algebra*, **324** (2010), 2464-2474.

[11] Henry H. Crapo, The Möbius Function of a Lattice, *Journal of Combinatorial Theory* **1** (1966), 126-131.

[12] Henry H. Crapo, Möbius Inversion in Lattices, *Archiv der Mathematik*, Birkhäuser Verlag, **19** (1968), 595-607.

[13] Francesca Dalla Volta and Andrea Lucchini, The A-Möbius function of a finite group, *ArXiv preprint*, 2021. arXiv:2109.05260v1 [math.GR]

[14] Francesca Dalla Volta and Giovanni Zini, On two Möbius functions for a finite non-solvable group, *Communications in Algebra* **49**, 4565-4576.

[15] C. D. Godsil, An Introduction to the Moebius Function, *ArXiv preprint*, 2018. arXiv:1803.06664v1 [math.CO]

[16] P. Hall, The Eulerian functions of a group, *Quarterly Journal of Mathematics* **7** (1936), 134–151.

[17] V. C. Harris and M. V. Subbarao, On Product Partitions of Integers, *Canadian Mathematical Bulletin* **34** (1991), 474-479.

[18] B. Hartley and T. O. Hawkes, *Rings, Modules and Linear Algebra*, Chapman and Hall, London, 1970

[19] T. Hawkes, I. M. Isaacs and M. Özaydin, On the Möbius function of a finite group. *Rocky Mountain Journal of Mathematics* **19** (1989), 1003-1034

[20] Laszlo Kalmar, Über die mittlere Anzahl der Produktdarstellungen der Zahlen. (Erste Mitteilung), *Acta Litterarum ac Scientiarum, Szeged* **5** (1931), 95-107.

[21] Peter Kleidman and Martin Liebeck, *The Subgroup Structure of the Finite Classical Groups*, Cambridge University Press, Cambridge, 1990.

[22] Oliver King, On Some Maximal Subgroups of the Classical Groups *Journal of Algebra* **68** (1981), 109-120.

[23] Charles Kratzer and Jacques Thévenaz, Fonction de Möbius d'un groupe fini et anneau de Burnside, *Comment. Math. Helvetici* **59** (1984), 425-438.

[24] Charles Kratzer and Jacques Thévenaz, Type d'homotopie des treillis et treillis des sous-groupes d'un groupe fini, *Comment. Math. Helvetici* **60** (1985), 85-106.

[25] Andrea Lucchini, The X-Dirichlet polynomial of a finite group, *Journal of Group Theory*, **8** (2005), 171-188.

[26] Andrea Lucchini, On the subgroups with non-trivial Möbius number, *Journal of Group Theory*, **13** (2010), 589-600.

[27] Avinoam Mann, Positively finitely generated groups, *Forum Mathematicum* **8** (1996), 429-459.

[28] Avinoam Mann, A probabilistic zeta function for arithmetic groups, *International Journal of Algebra and Computation*, **15** (2005), 1053-1059.

[29] James R. Munkres, *Elements of Algebraic Topology*, Westview Press - Perseus Publishing, Cambridge, Massachusetts, 1984.

[30] Peter M. Neumann and Cheryl E. Praeger, Cyclic matrices over finite fields, *Journal of the London Mathematical Society* (2) **52** (1995), 263-284.

[31] Peter M. Neumann and Cheryl E. Praeger, Cyclic Matrices in Classical Groups over Finite Fields, *Journal of Algebra* **234** (2000), 367–418.

[32] Nikolay Nikolov and Dan Segal, On finitely generated profinite groups, I: strong completeness and uniform bounds, *Annals of Mathematics* **165** (2007), 171-238.

[33] Herbert Pahlings, On the Möbius function of a finite group, *Archiv der Mathematik* **60**, (1993), 7-14.

[34] Luis Ribes and Pavel Zalesskii, *Profinite Groups*, Springer-Verlag, New York, 2000.

[35] Derek J. S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag, New York, 1993 (2nd ed., 1996).

[36] Gian-Carlo Rota, On the Foundations of Combinatorial Theory, I. Theory of Möbius Functions, *Z. Wahrscheinlichkeitsth.* **2** (1964), 340-368.

[37] Anna Katharina Schröder, *The maximal subgroups of the classical groups in dimension 13, 14 and 15*, Ph.D. Thesis, University of St Andrews, 2015.

[38] John Shareshian, *Combinatorial properties of subgroup lattices of finite groups*, Ph.D. Thesis, Rutgers - The State University of New Jersey, 1996.

[39] Mark Siggers, On the Representations of Finite Distributive Lattices, *Kyungpook Mathematical Journal* **60** (2020), 1-20.

[40] Stephen D. Smith, *Subgroup Complexes*, American Mathematical Society, Providence, Rhode Island, 2011

[41] Richard P. Stanley, *Enumerative Combinatorics, Volume I*, second ed., Cambridge University Press, Cambridge, 2012 (first ed. published by Wadsworth & Brooks/Cole, 1986).

[42] Donald E. Taylor, *The geometry of the classical groups*, Heldermann Verlag, Berlin, 1992

[43] G. E. Wall, Counting cyclic and separable matrices over a finite field, *Bulletin of the Australian Mathematical Society* **60** (1999) 253-284

[44] John S. Wilson, *Profinite Groups*, Clarendon Press, Oxford, 1998.

[45] Robert A. Wilson, *The Finite Simple Groups*, Springer-Verlag, London, 2009.